|  |  |  |
| --- | --- | --- |
|  | **Vital College (Pty) Ltd** | |
| Authorised by: | Duncan MacNicol |
|  | Date Authorised: | 20 February 2021 |
| C:\Users\JReddy\AppData\Local\Microsoft\Windows\INetCache\Content.Word\Vital small simple.jpg | Document Number: | VC - 001 |

**Technology Disposal Policy**

1. **Introduction**
2. **Overview**

Technology equipment often contains parts which cannot simply be thrown away.  Proper disposal of equipment is both environmentally responsible and often required by law. In addition, hard drives, USB drives and other storage media contain various kinds of Vital College data, some of which is considered sensitive.  In order to protect our data, all storage mediums must be properly erased before being disposed of.  However, simply deleting or even formatting data is not considered sufficient.  When deleting files or formatting a device, data is marked for deletion, but is still accessible until being overwritten by a new file.  Therefore, special tools must be used to securely erase data prior to equipment disposal.

1. **Scope**

This policy applies to any computer/technology equipment or peripheral devices that are no longer needed within Vital College including, but not limited to the following: computers, servers, hard drives, laptops, portable storage devices (i.e., USB drives), backup tapes. For printed materials, please refer to the **Document Management Policy and Procedure**. This policy does not apply to Solid State Drives, when files are deleted from a solid-state drive, they are permanently deleted with no chance of data recovery.

The purpose of this policy it to define the guidelines for the disposal of technology equipment and components owned by Vital College.

1. **Policy Statement**
2. **Technology Equipment Disposal**
3. all storage mediums.
4. All data including, all files and licensed software shall be removed from equipment using disk sanitizing software that cleans the media overwriting each and every disk sector of the machine with zero-filled blocks.
5. All electronic drives must be degaussed or overwritten with a commercially available disk cleaning program. Hard drives may also be removed and rendered unreadable (drilling, crushing or other demolition methods).
6. Technology equipment with non-functioning memory or storage technology will have the memory or storage device removed and the memory or storage will be physically destroyed.
7. **References**

|  |
| --- |
| **Document Name** |
| Document Management Policy and Procedure |
| Exceptions Policy |

1. **Outputs**

The following records need to be kept and stored securely.

|  |  |  |  |
| --- | --- | --- | --- |
| **Record** | **Responsible Person** | **Retention** | **Disposition** |
|  |  |  |  |
|  |  |  |  |

All records must be stored in the pre-allocation location. All physical copies need to be stored in a lockable cabinet or drawer.

1. **Enforcement**

An employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment. A violation of this policy by a temporary worker, contractor or vendor may result in the termination of their contract or assignment with Vital College.

Any exception to the policy must comply with the **Exceptions Policy**.

1. **Definitions**

|  |  |
| --- | --- |
| **TERMS** | **DESCRIPTION** |
|  |  |

A black and white drawing of a handwritten note

Description automatically generated with low confidence

**DIRECTOR name** Duncan MacNicol **DIRECTOR signature**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**Signed at** Durban **on this** 20th day of February 2021

|  |  |  |
| --- | --- | --- |
| C:\Users\JReddy\AppData\Local\Microsoft\Windows\INetCache\Content.Word\Vital small simple.jpg | **Vital College (Pty) Ltd** | |
| Authorised by: | Duncan MacNicol |
| Date Authorised: | 20 February 2021 |
| Document Number: | VC - 002 |

**Acceptable Use Policy**

1. **Introduction**
2. **Overview**

The purpose of this policy is to establish acceptable and unacceptable use of electronic devices and network resources at Vital College in conjunction with its established culture of ethical and lawful behavior, openness, trust, and integrity.

Vital College provides computer devices, networks, and other electronic information systems to meet missions, goals, and initiatives and must manage them responsibly to maintain the confidentiality, integrity, and availability of its information assets. This policy requires users of information assets to comply with company policies and protects the company against damaging legal issues.

1. **Scope**

All employees, contractors, consultants, temporary and other workers at Vital College, including all personnel affiliated with third parties, referred to as ‘users’ in this policy, must adhere to this policy. This policy applies to all information assets owned, operated and/or leased by Vital College, or to devices that connect to a Vital College network or reside at a Vital College site, referred to as “Vital College resources’ in this policy.

1. **Policy Statement**
2. **General Requirements**

All users are responsible for exercising good judgment regarding the appropriate use of Vital College resources in accordance with all Vital College policies, standards, and guidelines as applicable from time to time. Vital College resources may not be used for any unlawful or prohibited purposes.

For security, compliance, and maintenance purposes, authorized personnel may monitor and audit equipment, systems, and network traffic, and any use of the Vital College resources shall be regarded as being for business use. Devices that interfere with other devices or users on the Vital College network may be disconnected. Information Security prohibits actively blocking authorized audit scans. Firewalls and other blocking technologies must permit access to the scan sources.

1. **System Accounts**
2. Users are responsible for the security of data, accounts, and systems under the control of any user. All passwords must be kept strictly secure, and it is strictly prohibited to share account or password information with anyone, including other personnel, family, or friends. Providing access to another individual, either deliberately or through failure to secure its access, is a violation of this policy.
3. All users must maintain system-level and user-level passwords in accordance with the **Password Policy**.
4. Users must ensure through legal or technical means that confidential information always remains within the control of Vital College. Conducting Vital College business that results in the storage of confidential information on personal or non-Vital College controlled environments, including devices maintained by a third party with whom Vital College does not have a contractual agreement, is prohibited. This specifically prohibits the use of an e-mail account that is not provided by Vital College, or its customers and partners, for any company business.

1. **Computing Assets**
2. Users are responsible for ensuring the protection of assigned Vital College assets that includes the use of computer cable locks and other security devices. Laptops left at Vital College overnight must be properly secured or placed in a locked drawer or cabinet. Promptly report any theft of Vital College assets to the IT Department.
3. Where it comes to storage of Vital College equipment in transit in any vehicle, it is recommended that laptops always be kept in a boot if available. If the vehicle does not have a boot, then it is recommended that any laptop be pushed under the front seats. Laptops are not to be kept on vehicle seats, where they are visible and in direct sunlight.
4. All PCs, laptops, and workstations must be secured with a password-protected screensaver with the automatic activation feature set to 5 minutes or less.
5. All PCs, laptops, and workstations must be locked when left unattended.
6. All employees are personally responsible for the protection against damage of any computing asset, this includes liquid damage and physical damage to Vital College assets. The cost for the repair of any such asset will be recovered from the employees. An automatic deduction will be loaded on the employees next payslip to cover the cost for the insurance excess amount.
7. Devices that connect to the Vital College network must comply with the **Minimum Access Policy**.
8. Users must not interfere with corporate device management or security system software, including, but not limited to, Firewall, Antivirus, Encryption Software, Company Portal, and Monitoring system.
9. No asset tags, labels or other identifying markings may be removed from Vital College assets.
10. Users are responsible for keeping any computing asset for which the user is responsible is hygienically clean, in accordance with the guidelines in this document.
11. On return of any Vital College assets, any costs due to physical damage or lost peripherals will recouped from the user, which includes a deduction from the salary of the user where the user is an employee of Vital College.

1. **Network Use**

Users are responsible for the security and appropriate use of Vital College network resources under control of the user. Using the Vital College resources for any of the following is strictly prohibited:

1. Causing a security breach to either Vital College or other network resources, including, but not limited to, accessing data, servers, or accounts to which the user is not authorized; circumventing user authentication on any device or sniffing network traffic.
2. Causing a disruption of service to either Vital College or other network resources, including, but not limited to, ICMP floods, packet spoofing, denial of service, heap or buffer overflows, and forged routing information for malicious purposes.
3. Introducing honeypots, honeynets, or similar technology on the Vital College network.
4. Violating copyright law, including, but not limited to, illegally duplicating, or transmitting copyrighted pictures, music, video, and software. Users are required to familiarize themselves with the **Companies and Intellectual Property Commissions Copyright Policy**for additional information on copyright restrictions. This policy can be found on the CIPC website.
5. Exporting or importing software, technical information, encryption software, or technology in violation of international or regional export control laws. Users are required to familiarize themselves with the **Exception Policy** for additional information on export and transfer restrictions.
6. Use of the Internet or Vital College network that violates the **Acceptable Use Policy**, Vital College policies, or local laws.
7. Intentionally introducing malicious code, including, but not limited to, viruses, worms, Trojan horses, e-mail bombs, spyware, adware, and keyloggers.
8. Port scanning or security scanning on a production network unless authorized in advance by the IT department.

1. **Electronic Communications**

It is important to ensure that confidential information stays confidential, and every Person has the responsibility to ensure that our information and our clients information remains secure. We have created the **Information Classification Policy** in order to ensure that classified information is not accidentally shared with unauthorised parties, please refer to the **Information Classification policy** for more information.

The following shall however be strictly prohibited:

1. Inappropriate use of communication equipment, including, but not limited to, supporting illegal activities, and procuring or transmitting material that violates Vital College policies against harassment or the safeguarding of restricted or confidential information.
2. Sending Spam via e-mail, text messages, pages, instant messages, voice mail, or other forms of electronic communication.
3. Forging, misrepresenting, obscuring, suppressing, or replacing a user identity on any electronic communication to mislead the recipient about the sender.
4. Posting the same or similar non-business-related messages to large numbers of Distribution groups.
5. Use of a Vital College e-mail or IP address to engage in conduct that violates Vital College (Pty) Ltd policies or guidelines. Posting to a public newsgroup, bulletin board, or social media with a Vital College e-mail or IP address represents Vital College to the public bay be construed by third parties to represent the views of the company. Therefore, all users must exercise good judgment to avoid creating any adverse impression of the company by third parties, misrepresenting or exceeding the authority of the user in representing the opinion of the company or bringing the company name or brand into disrepute.
6. Users must not send emails with multiple clients in the To field. This exposes clients email addresses to other parties.
7. Sending emails to a large number of recipients is allowed, but only if the content has been reviewed and approved by a responsible manager.
8. The forwarding of any document / attachment / interesting article etc, is not permitted unless:

1. The user has actually first read it himself or herself; and
2. The user has verified the authenticity / integrity of the source / document; and
3. The user briefly summaries the key points; and
4. The user references what part of the document is of interest and what constitutes the key point the user intended to share; and
5. It is highlighted why the user found it relevant / applicable to the targeted audience.

1. Access to, receipt of, and any distribution or forwarding of any pornographic, racist, or discriminatory material of any nature whatsoever is strictly prohibited.

1. **References**

|  |
| --- |
| **Document Name** |
| Exception Policy |
| Minimum Access Policy |
| Password Policy |
| Information Classification Policy |
| Companies and Intellectual Property Commissions Copyright Policy |

1. **Outputs**

The following records need to be kept and stored securely.

|  |  |  |  |
| --- | --- | --- | --- |
| **Record** | **Responsible Person** | **Retention** | **Disposition** |
|  |  |  |  |
|  |  |  |  |

All records must be stored in the pre-allocation location. All physical copies need to be stored in a lockable cabinet or drawer.

1. **Enforcement**

An employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment. A violation of this policy by a temporary worker, contractor or vendor may result in the termination of their contract or assignment with Vital College (Pty) Ltd.

Any exception to the policy must comply with the **Exceptions Policy**.

1. **Definitions**

|  |  |
| --- | --- |
| **Terms** | **Description** |
| **Computing Asset** | An asset is any device, or other component of the environment that supports information-related activities, such as Laptops, Desktops, Monitors, Mouses, Keyboards, Mobile Phones, Routers, Switches, Servers, etc. |

A black and white drawing of a handwritten note

Description automatically generated with low confidence

**DIRECTOR name** Duncan MacNicol **DIRECTOR signature**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**Signed at** Durban **on this** 20th day of February 2021



|  |  |  |
| --- | --- | --- |
|  | **Vital College (Pty) Ltd** | |
| Authorised by: | Duncan MacNicol |
| Date Authorised: | 20 February 2021 |
| Document Number: | VC-003 |

**Backup and restore Policy**

1. **Introduction**
   1. **Overview**

Vital College has a duty to ensure that all information and data which it is responsible for is securely and routinely backed up. The company has a responsibility to ensure that the information and data which has been backed up can be restored in the event of deletion, loss, corruption, and damage or made unavailable due to unforeseen circumstances. The purpose of this policy is to identify and establish processes, procedures, and good working practices for the backup and timely recovery of the company’s information and data, existing in both electronic and physical form.

* 1. **Scope**

All employees, contractors, consultants, temporary and other workers at Vital College, including all personnel affiliated with third parties must adhere to this policy. This policy applies to information assets owned or leased by Vital College, or to devices that connect to a Vital College network or reside at an Vital College site.

The scope of this policy extends to the back-up of important information and data, regardless of the form it takes including the recovery of IT systems and supporting infrastructure.

1. **Policy Statement**
   1. **General Requirements**

There is always a risk that systems and/or procedures will fail resulting in loss of access to information, data and systems, despite the implementation of best practice.

The following steps will help ensure Vital College information and data is backed up and restored securely in the most efficient manner possible.

1. **Data Backups**
   * 1. Vital College IT administrators are responsible for providing system support and data backup tasks and must ensure that adequate backup and system recovery practices, processes and procedures are followed in line with the company’s **Business Continuity Policy**.
     2. All IT backup and recovery procedures must be documented, regularly reviewed, and made available to trained personnel who are responsible for performing data and IT system backup and recovery.
     3. All infrastructure state data on the servers including servers, networking, and supporting system configuration files must be systematically backed up in the event of system re-installation and/or configuration.
     4. All backup media must be encrypted and appropriately labelled with date/s and codes/markings which enables easy identification of the original source of the data and type of backup used on the media. All encryption keys should always be kept securely in accordance with the **Acceptable Encryption Policy**.
     5. A recording mechanism must be in place and maintained to record all backup information such as date, backup details (i.e. Server Name) including any failures or other issues relating to the backup job.
     6. Backup media which is retained on-site prior to being sent for storage at a remote location must be stored securely and ensure both the original and backup copies are stored in separate physical locations.
     7. Access to the on-site backup location must be restricted to authorised personnel only. Please refer to the **Server Room Access Information** document.
     8. All backups identified for long term storage must be stored at a remote secure location with appropriate environmental control and protection to ensure the integrity of all backup media.
     9. Hard copy paper files containing important information and data should be scanned and stored electronically to ensure digital copies are created which can be backed up by the company’s ICT systems. Where this may not be possible, photocopies of paper files must be made and stored in a secure storage location.
     10. Regular tests must be carried out to establish the effectiveness of the company’s backup and restore procedures by restoring data/software from backup copies and analysing the results. Vital College IT Manager should be provided with the information relating to any issues that may arise while testing the restored data.
     11. The IT Administrators should notify the IT Manager when backups fail – providing information such as the backup job detail and reasons (if applicable) for the failure. A record must be maintained, detailing the backup job failure including any actions taken.
     12. Backup data/media no longer required must be clearly marked and recorded for secure disposal and with due environmental consideration.
2. **User responsibilities**

Users also have a responsibility to ensure Vital College data is securely maintained and is available for backup.

* + 1. Users must not store any data/files on the local drive of a computer (this excludes the normal functioning of the Windows operating system and other authorised software which requires the ‘caching’ of files locally in order to function). Instead, Users must save data (files) on their allocated areas. Data (files) which are stored “locally” will NOT be backed up and will therefore be at risk of exposure, damage, corruption, or loss.
    2. If the company network becomes unavailable for whatever reason and data or work is at risk of being lost, users may have no option but to save the data (files) locally (i.e., on the computer being used) or on approved media storage such as a company owned encrypted Data stick (USB storage). Once the Corporate Network becomes available again, data (files) should be immediately transferred to the corporate network for it to be backed up safely and local copies of data on the computer or portable storage media must be deleted. This will help to ensure the availability and integrity of data and to avoid duplicate copies of data being stored.
    3. Please refer to the **Removable Media Policy** for acceptable standards when backing up data to removable storage.
    4. Mobile phones can be used to store sensitive, business, or personal identifiable information, but mobile phones will have to comply with the **Minimum Access Policy**.

1. **Data Restores**

Data (file) restores are carried out by the Vital College IT Team who will endeavour to restore files from a date specified by the user or from the nearest backed up date.

* + 1. Users must request data (files) to be restored by contacting the Internal IT Department. Only files which the user is authorised to access will be provided from the restore.
    2. The Internal IT Department will need to verify that the User has permission and/or authorisation to view or obtain restored copies of file/s and/or folder/s.
    3. Users requesting a restore/s are required to provide as much information about the data (file/s) as necessary – this will include:
    - The reason for the restore.
    - The name of file/s and/or folder/s and/or system/s to be restored.
    - Date, day or time of deletion/corruption or nearest approximation.
    - The last date, day or time which the User recalls the data (files) being intact and accessed/used successfully.
    1. All backup and recovery (restore) procedures must be documented and made available to Vital College IT for carrying out data (file) restores.
    2. Requests from third party software/hardware vendors for file or system restores for the purpose of system support, maintenance, testing, or other unforeseen circumstance should be made under the supervision of the IT Manager, CIO or an Vital College representative appointed by the IT Manager or CIO.
    3. Personnel accessing backup media for the purpose of a restore must ensure that any media used is returned to a secure location when no longer required.

1. **References**

|  |
| --- |
| **Document Name** |
| Business Continuity Policy |
| Acceptable Encryption Policy |
| Server Room Access Information |
| Removable Media Policy |
| Minimum Access Policy |
| Exceptions Policy |

1. **Outputs**

The following records need to be kept and stored securely.

|  |  |  |  |
| --- | --- | --- | --- |
| **Record** | **Responsible Person** | **Retention** | **Disposition** |
| Backup Report | IT Manager | 12 Months | Archive / Delete |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

All records must be stored in the pre-allocation location. All physical copies need to be stored in a lockable cabinet or drawer.

**Enforcement**

An employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment. A violation of this policy by a temporary worker, contractor or vendor may result in the termination of their contract or assignment with Vital College.

Any exception to the policy must comply with the **Exceptions Policy**.

**Definitions**

|  |  |
| --- | --- |
| **Terms** | **Description** |
| **Infrastructure state data** | This generally refers to data in a database or file that functions as system, application, user or backup data. Such data is physically stored on a data storage device such as a hard drive that may be located locally or on remote infrastructure such as a cloud service. |
| **Backup media** | Storage media, these are devices that store application and user information. The primary storage media for a computer is usually the internal hard drive. The secondary storage media is usually referred to as the backup media, a removable hard drive, USB flash Drive, Tape Drive, Cloud Drive. The secondary storage media usually contains copies of the information stored on the primary storage media. |
| **Encryption** | The process of converting information or data into a code, especially to prevent unauthorized access. |

A black and white drawing of a handwritten note

Description automatically generated with low confidence

**DIRECTOR name** Duncan MacNicol **DIRECTOR signature**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**Signed at** Durban **on this** 20th day of February 2021

|  |  |  |  |
| --- | --- | --- | --- |
| C:\Users\JReddy\AppData\Local\Microsoft\Windows\INetCache\Content.Word\Vital small simple.jpg | **Vital College (Pty) Ltd** | | |
| Authorised by: | Duncan MacNicol |
| Date Authorised: | 20 February 2021 |
| Document Number: | VC - 004 |

**Change management and control Policy**

1. **Introduction**
   1. **Overview**

Operational change management brings discipline and quality control to Information Security. Attention to governance and formal policies and procedures will ensure its success. Adopting formalized governance and policies for operational change management delivers a more disciplined and efficient infrastructure. This formalization requires communication; the documentation of important process workflows and personnel roles; and the alignment of automation tools, where appropriate. Where change management is non-existent, it is incumbent on Information Security’s senior management to provide the leadership and vision to jump-start the process. By defining processes and policies, Information Security organizations can demonstrate increased agility in responding predictably and reliably to new business demands.

Vital College management has recognized the importance of change management and control and the associated risks with ineffective change management and control and have therefore formulated this Change Management and Control Policy in order to address the opportunities and associated risks. The purpose of this policy is to establish management direction and high-level objectives for change management and control. This policy will ensure the implementation of change management and control strategies to mitigate associated risks such as:

• Information being corrupted and/or destroyed;

• Computer performance being disrupted and/or degraded;

• Productivity losses being incurred; and

• Exposure to reputational risk.

* 1. **Scope**

This policy applies to all parties operating within the Vital College network environment or utilizing Information Resources. It covers the Servers, Networking equipment, Policies and Procedures located at Vital College offices and Vital College production related locations, where these systems are under the jurisdiction and/or ownership of the Vital College or subsidiaries.

Development changes to the Vital College system has a separate change control process. Details about the process is documented in the **Software Development Lifecycle (SDLC)** policies.

1. **Policy Statement**
   1. **Preamble**
      1. Changes to information resources shall be managed and executed according to a formal change control process. The control process will ensure that changes proposed are reviewed, authorised, tested, implemented, and released in a controlled manner; and that the status of each proposed change is monitored.
      2. In order to fulfil this policy, the following statements shall be adhered to:
   2. **Operational Procedures**
      1. The change control process shall be formally defined and documented. A change control process shall be in place to control changes to all Vital College information resources
   3. **Document Change**
      1. All change requests shall be stored whether approved or rejected. The approval of all change requests and the results thereof shall be documented on the RFC Request for Change document.
      2. A documented audit trail containing relevant information shall always be maintained. This should include change request documentation, change authorisation and the outcome of the change. No person should implement changes to production information systems without the approval of other authorised personnel.
   4. **Change Classification**
      1. All change requests shall be prioritized in terms of benefits, urgency, effort required and potential impact on operations. This will be documented on the Request for Change document.
   5. **Testing**
      1. Changes shall be tested in an isolated, controlled, and representative environment (where such an environment is feasible) prior to implementation to minimize the effect on the relevant business process, to assess its impact on operations and security and to verify that only intended and approved changes were made.
   6. **Approval**
      1. All changes shall be approved prior to implementation. Approval of changes shall be based on formal acceptance criteria i.e. the change request was done by an authorized user, the impact assessment was performed, and proposed changes were tested.
   7. **Implementation**
      1. Implementation will only be undertaken after appropriate testing and approval by stakeholders.
   8. **Fall Back**
      1. Procedures for aborting and recovering from unsuccessful changes shall be documented. Should the outcome of a change be different to the expected result (as identified in the testing of the change), procedures and responsibilities shall be noted for the recovery and continuity of the affected areas. Fall back procedures will be in place to ensure systems can revert to what they were prior to implementation of changes.
   9. **Documentation**
      1. Information resources documentation shall be updated on the completion of each change and old documentation shall be archived or disposed of as per Vital College data retention policies.
   10. Information resources documentation is used for reference purposes in various scenarios i.e. further development of existing information resources as well as ensuring adequate knowledge transfer in the event of the original developer and/or development house being unavailable. It is therefore imperative that information resources documentation is complete, accurate and kept up to date with the latest changes.
   11. **Business continuity Plans (BCP)**
       1. Business continuity and Disaster recovery plans shall be updated with relevant changes, managed through the change control process. Business continuity plans rely on the completeness, accuracy, and availability of BCP documentation. BCP documentation is the road map used to minimize disruption to critical business processes where possible, and to facilitate their rapid recovery in the event of disasters.
   12. **Emergency Changes**
       1. Specific procedures to ensure the proper control, authorization, and documentation of emergency changes shall be in place. Specific parameters will be defined as a standard for classifying changes as Emergency changes.
   13. **Change Monitoring**
       1. All changes will be monitored once they have been rolled-out to the production environment. Deviations from design specifications and test results will be documented and escalated to the solution owner for ratification.

**References**

|  |
| --- |
| **Document Name** |
| SDLC Software Development Lifecycle |
| System change control |
|  |
|  |
|  |
|  |

**Outputs**

The following records need to be kept and stored securely.

|  |  |  |  |
| --- | --- | --- | --- |
| **Record** | **Responsible Person** | **Retention** | **Disposition** |
| Request For Change | IT Manager | 12 Months | Delete / Archive |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

All records must be stored in the pre-allocation location. All physical copies need to be stored in a lockable cabinet or drawer.

**Enforcement**

An employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment. A violation of this policy by a temporary worker, contractor or vendor may result in the termination of their contract or assignment with Vital College.

Any exception to the policy must comply with the **Exceptions Policy**.

A black and white drawing of a handwritten note

Description automatically generated with low confidence**Definitions**

|  |  |
| --- | --- |
| **TERMS** | **DESCRIPTION** |
|  |  |

**DIRECTOR name** Duncan MacNicol **DIRECTOR signature**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**Signed at** Durban **on this** 20th day of February 2021

|  |  |  |
| --- | --- | --- |
|  | **Vital College (Pty) Ltd** | |
| C:\Users\JReddy\AppData\Local\Microsoft\Windows\INetCache\Content.Word\Vital small simple.jpg | Authorised by: | Duncan MacNicol |
| Date Authorised: | 20 February 2021 |
| Document Number: | VC-005 |

**Clean Desk Policy**

1. **Introduction**
   1. **Overview**

A clean desk policy can be an important tool to ensure that all sensitive/confidential materials are removed from an end-user workspace and locked away when the items are not in use or an employee leaves his/her workstation. It is one of the top strategies to utilize when trying to reduce the risk of security breaches in the workplace. Such a policy can also increase employee’s awareness about protecting sensitive information.

* 1. **Scope**

This policy applies to all parties operating within the Vital College network environment or utilizing Information Resources. It covers the data networks, servers, and personal computers (stand-alone or network-enabled), located at Vital College offices, employee home office, and Vital College production-related locations, where these systems are under the jurisdiction and/or ownership of the Vital College or subsidiaries, and any personal computers, laptops, mobile device and or servers authorized to access Vital College data networks.

A Clean Desk policy is not only ISO 27001/17799 compliant, but it is also part of standard privacy controls.

1. **Policy Statement**
   1. **Generic Requirements**
      1. Employees are required to ensure that all sensitive/confidential information in hardcopy or electronic form is secured in a confidential and safe place in their work area at the end of the day and when they are expected to be absent for an extended period.
      2. Computer workstations must be screen locked when the workspace is unoccupied.
      3. Computer workstations must be shut completely down at the end of the workday.
      4. File cabinets containing Restricted or Sensitive information must be kept closed and locked when not in use or when not attended.
      5. Keys and access cards used for access to Restricted or Sensitive information must not be left unattended.
      6. Laptops must be either locked with a locking cable or locked away in a drawer.
      7. Passwords may not be left on sticky notes posted on or under a computer, nor may they be left written down in any form in an accessible location.
      8. Printouts containing Restricted or Sensitive information, as defined in the Information Classification Policy should be immediately removed from the printer.
      9. Upon disposal, Confidential and/or Restricted documents should be shredded in the official shredder bins or placed in the lock confidential disposal bins.
      10. All meeting room whiteboards must be cleaned after every meeting.
      11. Lock away unattended portable computing devices such as laptops and tablets.
      12. Treat mass storage devices such as CDROM, DVD, or USB drives as sensitive and secure them in a locked drawer.
      13. All printers and fax machines should be cleared of printed papers as soon as they are printed, this helps ensure that sensitive documents are not left on printer trays for the wrong person to pick up.
      14. All shared printers must be secured with user PIN codes.

**References**

|  |
| --- |
| **Document Name** |
| Exceptions Policy |
| Information Classification Policy |
|  |
|  |
|  |
|  |

**Outputs**

The following records need to be kept and stored securely.

|  |  |  |  |
| --- | --- | --- | --- |
| **Record** | **Responsible Person** | **Retention** | **Disposition** |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

All records must be stored in the pre-allocation location. All physical copies need to be stored in a lockable cabinet or drawer.

**Enforcement**

An employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment. A violation of this policy by a temporary worker, contractor or vendor may result in the termination of their contract or assignment with Vital College.

Any exception to the policy must comply with the **Exceptions Policy**.

**Definitions**

|  |  |
| --- | --- |
| **TERMS** | **DESCRIPTION** |
| **ISO 27001/17799** | This is an information security standard, part of the ISO/IEC 27000 family of standards, of which the last version was published in 2013, with a few minor updates since then. |

A black and white drawing of a handwritten note

Description automatically generated with low confidence

**DIRECTOR name** Duncan MacNicol **DIRECTOR signature**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**Signed at** Durban **on this** 20th day of February 2021



|  |  |  |
| --- | --- | --- |
|  | **Vital College (Pty) Ltd** | |
| Authorised by: | Duncan MacNicol |
| Date Authorised: | 20 February 2021 |
| Document Number: | VC-006 |

**Data first touch Policy**

1. **Introduction**
   1. **Overview**

This document sets out the guidelines and minimum procedural considerations necessary to ensure that all data received, collated, and transferred are done safe, secure, and in compliance with the best practices of the Vital College Group.

* 1. **Scope**

This document covers all forms of first touch data, whether electronic nature, hard copy, hard drive and or other verbal information reworded into formal script / electronic copy. This document will cover all aspects from receipting, collation, transit, handover, and safeguarding within the safe zones.

1. **First Touch & Data Collection Principles** 
   1. **Fundamental Principles of taking receipt of information/data**

* Data Classification
* Consent / Permission from the data subject
* Data Registration
* Data Classification Risk
* Data Accuracy and Completeness
* Data Storage / Transfer or Discarding Assessment
* Data Storage Format
* Data Transfer Requirements
  + Physical Documents
  + Electronic Data
  + Verbal Data
  + Visual Data
* Data Discarding Protocol
* Data Archiving Requirements
* Data Retrieval Process
* Data revisit and continuous update
* Data breach protocol
  + 1. **Classification Data Subjects consent to retain, hold and collect information**

The primary consideration before accepting data from any source is to assess whether the data obtained is of a personal, confidential, and or private nature. This will enable you to assess whether the necessary steps following must be adhered to, as **POPI and Privacy Policy** only apply to such information. Please see **Information Classification Policy and Procedure** for classification requirements.

* + 1. **Consent / Permission from the data subject**

Before accepting any confidential, personal, and/or private information, it is of utmost importance to ensure that you have the written consent and permission of the data subject to keep, transfer, pass on, distribute, use, or store such information.

If no such consent or permission can be obtained or reasonably ascertained, then the data must be returned with immediate effect as per the **POPI and Privacy Policy**.

Methods to obtain such permission or consent include but are not limited to the following means:

* Letter of consent
* Data collection forms
* Email consent
* Public website downloads (publishing)
* Contractual Agreements and Non-Disclosure Agreements
* Recorded verbal consent
* SMS consent from a verifiable contact source
* Other legal permission of written consent

What will not be deemed as valid consent:

* Any form of consent whereby the data subject cannot be identified in the consent
* Any form of verbal / written consent on behalf of a data subject, without evidence of the data subject’s consent or proxy
* Any form of verbal/visual consent whereby it is not recorded and whereby the data subject cannot be identified on any such recording
  + 1. **Data acceptance registration**

Upon receiving confidential, personal, or private data from such subjects, it is mandatory to record the receipt of such data on a register in the following instances:

* When collecting the data in person
* When collecting the data using a courier
* When collecting the data in a physical format such as:
  + Physical paper documents
  + Physical hard drives/storage devices

What must be captured on this register document:

* An exact description of documents or information received
* Information classification (As per the **Information Classification Policy and Procedure**)
* Number of documents received
* Type of file or document (paper, hard drive, etc)
* Permission to store / keep or hold information (Refer to section 2.1.2 Consent / Permission from the data subject)
* Signed by the data custodian (Track change)

For this reason, it is strongly advised that all client and supplier data be sent to or collected from a central contact point and central data collection email, that can be encrypted, securely manned, and monitored.

* + 1. **Data Accuracy and Completeness**

All data collected must serve a purpose and must be of future or current use (Relevance). If not, there is no justification for keeping such information, data discarding must be considered. All data that are to be used therefore must be accurate, complete, and up to date. It is extremely important to verify the source, accuracy, and completeness of data directly with the subject matter and where possible with an external confidential bureau’s where and when permitted by data subject to do so.

It is further recommended that all data be verified and reviewed within the intervals specified in the **Legislation Compliance Register** for changes, revisions, and or outdated compliance certificates where applicable.

* + 1. **Data Storage, Transfer or Discarding Assessment**

When considering taking ownership of data, it is very important to plan the data flow and movement from yourself as the data custodian till ultimate data safeguarding in a “secure safe zone” environment.

This process involves:

* taking ownership of the data and becoming the initial data custodian
* transferring or immediately storing the data to a “safe secure zone”
* distributing or passing off the data between data end-users
* eventual discarding of the data / archiving data

Upon taking receipt and ownership of data (data custodian owns the risk), it is of utmost importance to ensure that the necessary storage facilities/platform and/or requirements are identified and in place to safeguard and secure all confidential, personal, or private information from receipting through till ultimate destruction or data discarding and after.

Such storage should ensure proper access controls, proper data registration of movements or transfers as well as enable easy data retrieval and destruction/discarding.

As to assist in such assessments, Name has established a “Secure Safe Zone” storage facility in that we have:

* Access controlled servers’ storage (Electronic files)
* Access controlled Server Rooms (Hardware)
* Access controlled Storage Rooms (Physical Document room)
* Access controlled Offices (Meetings, Documents & IT equipment)
* Access controlled finance offices/upper-level access
* Data retrieval and storage policies
* Data archiving ISO27001 compliant service partnerships with our Archiving and Filing Service Provider
* Access controlled mail servers

Due to the above, it is essential to assess and identify the storage method and needs upfront, as to enable the best practices and fastest secure route to storage and safeguarding of confidential, personal, and private information.

For this reason, it is strongly advised that all client and supplier data be sent to or collected from a central contact point and central data collection email, that can be encrypted, securely manned, and monitored. To further control or mitigate this risk area, the next sections deal with the storage formats and data movement between or to a “safe secure zone”.

* + 1. **Data Storage Format**

The following hierarchy of preferred data storage is permitted by the Vital College group:

* Electronic data (PDF, Word, Excel, PPT) on official Vital College Access controlled servers
* Electronic data (PDF, Word, Excel, PPT) on a password protected and encrypted Vital College computer devices
* Physical Server Rooms for IT hard drives, storage drive, and servers
* Physical Financial Statements / Data within the finance secure offices (CFO locked office)
* Physical Supplier Statements within finance secure offices
* Physical Business Continuity Plan / IT Disaster Recovery Plan (Filed in DIRECTOR / COO & CIO Secure office)
* Physical files stored in secure product offices and archived.

It is Vital College best practice to minimize and prevent physical document storage as far as humanly possible. It is recommended that all information be scanned, converted to electronic format as quickly and as soon as possible during the information life cycle. All physical documents must be limited and if legally required, then such must be stored at Vital College “safe secure zone” as immediately as possible after initial receipt or generation of such documents/reports.

Information on removable hard drives, external storage devices must adhere to the information technology security practices as prescribed under the **Removable Media Policy**.

* 1. **Data Transfer Requirements and Protocol (Data in Transit)**

When data must be transferred between two “safe secure zones”, all protocols to limit exposure of a data breach must be followed, during such transfer phase. Which include but are not limited to the following:

* Limit trips from collection source (client/supplier) to Safe Secure Zone storage point (No personal or unneeded trips or stops)
* Do not store the documents in the plain or open site during transit
* Ensure documents are placed in a lockable bag, suitcase, or backpack that has a hidden Zip locks setup
* When using private transport, ensure documents are kept in a lockable rear boot of a car, or underneath the seat where not possible as to limit visibility.
* When using public transport, ensure that the bag with information is controlled and held at all times and not out of reach or sight.
* Ensure that your bag, luggage is in sight at all times and never left unattended.
* When reaching the “Safe Secure Zone”, prioritize handover of information as follows:
  + Direct actions towards handing over as soon and smoothly as possible
  + Ensure that all data is handed over, stored, and filed per the filing requirements.
  + Ensure that where applicable the register and/or Share drive folder is updated with the information placed in it.
  + Ensure that information handed over is stored in such a manner that it can be retrieved.

Confidential, personal, and or private information, may not be moved, transferred, without a formal movement register.

For this purpose, all documents will be recorded on a **Movement Register** and the location will be indicated as and when removed, replaced, or discarded.

* 1. **Data Discarding**

When data no longer serves any purpose or no longer has a use, it is mandatory to discard such data or information. This is to limit any potential data breach exposure and losses to our business resulting from such risks.

When during the discarding phase, it is discovered that data still hold potential future benefits use or needs, the best practice is to formally Archive such data files.

When discarding data, the rules and guidelines set out under the Data **Disposal and Destruction Policy** must be adhered to.

* 1. **Data Archiving**

Due to the risk and costs associated with storing physical documents, it is extremely important to apply the following guidelines in assessing whether data is ready to be archived or whether there is an actual need to archive, above destruction or discarding. These considerations and guidelines include, but are not limited to:

* SAICA’s guidelines with regards to document retention timeframes as well as our internal document retention policies.
* Frequency of revisiting the physical stored documents
  + If frequent remain onsite
* The lifespan of the document and the period it relates to
  + Prior year; archive
  + Older than retention requirements; destruct
  + No value/use left then destruct
* Nature of the document and risk associated if not immediately available
  + High risk; on-site
  + Moderate risk; on-site
  + No risk; off-site archive
* Legal requirements with regards to original documents
  + If legally needed, consider it must be kept:
    - at Registered office
    - at Auditors / Secretary / Lawyers Offices
  + If not legally needed, consider the above points
* The need for an actual hard copy or original documents
  + If needed; refer to the above guidelines
  + No need; refer to destruction/discarding
* Onsite storage space
* Offsite storage compliance and cost

It remains the Head of each product department and support service department to annually assess what documents are in the archive and which documents must be purged and discarded under the guideline of the **Disposal and Destruction Policy**.

Refer to the Document Retention policy for guidelines on archiving and unarchiving practices.

* 1. **Data Retrieval**

When data is initially stored, it must be done in such a way, that it can easily be tracked, traced, and retrieved upon request. As to ensure that data retrieval is done by only valid, permitted, and authorized users, data/information must always be stored in line with the **Information Classification Policy.**

Data retrieval includes the following as mere examples:

* Re-access by the custodian after the initial storage
  + Original user
  + Other users
* Return of document to the custodian from “safe secure zone”:
  + Within “safe secure zone”
  + Outside of the “safe secure zone”
* Extraction of data from emails / online secure servers
* Tracking the location of the data and verifying location is still relevant (Maintaining of, for example, a Document Register)

When accessing data on our secure online servers, the system maintains activity logs.

When documents or files are removed from the “Safe Secure Zone” then refer to point 2.1.4 above. Consider the following protocol:

* Update the register in 2.1.4 above to identify and track which user accessed what documents and where the location will be during such use.
* Weekly the register must be reviewed for any documents that have not been returned and that are outstanding.
* When documents have been unreturned after multiple weeks, the HOD must investigate and justify the cause.

Special care must be taken when documents/files leave the “Safe secure Zone” and the following protocols must be followed:

* If the documents are extremely confidential / highly important:
  + It must be kept behind lock and key when the custodian cannot return to the primary file location in a safe secure zone
  + The documents may not be displayed or left in the open
  + The documents may not be stored or left in an open office overnight / during break
  + The document may not leave the primary office, without approval from HOD and
    - Without proper transit protocol
    - Without arranged safeguarding
    - Without signing the document register
    - Without ensuring scanned copy (back-up) on file
* If the documents are not of high risk or high confidentiality:
  + The control must be maintained over the document
  + Alterations must be tracked
  + It must be returned as soon as possible after use
  + **Clean Desk Policy** must be adhered to
  1. **Data Revisit and Continuous Update**

When data is collected from an external data subject and frequently used or shared or of a personal/private nature, it is the responsibility of the data custodian to ensure that the data used, held in possession is accurate and up to date and does not cause any disrepute to the data subject. For illustrative purposes, the below example is provided as a guide:

Data subject A provides Vital College with their confidential financial trade references. This might be accurate and relevant for a fixed period. However, as time passes, data subject A’s credit rating changes. If Vital College neglected to update such information, and it still provides references on the original data, we as Vital College would cause harm or disrepute to the data subject or users permitted by the data subject.

For these reasons, it is highly advised to annually review client and supplier data for integrity and relevance.

* 1. **Data Breach**

When a user suspects that there has been a breach in data access, confidentiality, or private information has escaped the secure zone to unauthorized users, such a user should follow the steps defined within the **Incidents and Non-Conformance Procedure.**

**References**

|  |
| --- |
| **Document Name** |
| ISO27001 |
| SAICA – Document Retention Guidelines |
| Company Act 71 of 2008 |
| Disposal and Destruction Policy |
| Legislation Compliance Register |
| POPI and Privacy Policy |
| Information Classification Policy and Procedure |
| Legislation Compliance Register |
| Removable Media Policy |
| Clean Desk Policy |
| Incidents and Non-Conformance Procedure |

**Outputs**

|  |  |  |  |
| --- | --- | --- | --- |
| **Record** | **Responsible Person** | **Retention** | **Disposition** |
| Document Register | Storeroom | Indefinite | N/a |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

The following records need to be kept and stored securely.

All records must be stored in the pre-allocation location. All physical copies need to be stored in a lockable cabinet or drawer.

**Enforcement**

An employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment. A violation of this policy by a temporary worker, contractor, or vendor may result in the termination of their contract or assignment with Vital College.

A black and white drawing of a handwritten note

Description automatically generated with low confidenceAny exception to the policy must comply with the **Exceptions Policy**.

**DIRECTOR name** Duncan MacNicol **DIRECTOR signature**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**Signed at** Durban **on this** 20th day of February 2021

|  |  |  |
| --- | --- | --- |
|  | Vital College (Pty) Ltd | |
| Authorised by: | Duncan MacNicol |
| Date Authorised: | 20 February 2021 |
| Document Number: | VC-007 |



**Database credentials Policy**

1. **Introduction**
   1. **Overview**

Database authentication credentials are a necessary part of authorizing application to connect to internal databases. However, incorrect use, storage and transmission of such credentials could lead to compromise of very sensitive assets and be a springboard to wider compromise within the organization.

* 1. **Scope**

This policy is directed at all system implementer and/or software engineers who may be coding applications that will access a production database server on the Vital College Network. This policy applies to all software programs, modules, libraries or APIS that will access a Vital College, multi-user production database. It is recommended that similar requirements be in place for non-production servers and lab environments since they don’t always use sanitized information

This policy states the requirements for securely storing and retrieving database usernames and passwords (i.e., database credentials) for use by a program that will access a database running on one of Vital College networks.

Software applications running on Vital College networks may require access to one of the many internal database servers. In order to access these databases, a program must authenticate to the database by presenting acceptable credentials. If the credentials are improperly stored, the credentials may be compromised leading to a compromise of the database.

1. **Policy Statement**
   1. **General Requirements**

In order to maintain the security of Vital College internal databases, access by software programs must be granted only after authentication with credentials. The credentials used for this authentication must not reside in the main, executing body of the program's source code in clear text. Database credentials must not be stored in a location that can be accessed through a web server.

* 1. **Specific Requirements**

Storage of Data Base Usernames and Passwords:

* + 1. Please refer to the **Secure Coding Policy** for guidance on the coding practice standards used within Vital College.
    2. Database usernames and passwords may be stored in a file separate from the executing body of the program's code. This file must not be world readable or writeable.
    3. Database credentials may reside on the database server. In this case, a hash function number identifying the credentials may be stored in the executing body of the program's code.
    4. Database credentials may be stored as part of an authentication server (i.e., an entitlement directory), such as an LDAP server used for user authentication. Database authentication may occur on behalf of a program as part of the user authentication process at the authentication server. In this case, there is no need for programmatic use of database credentials.
    5. Database credentials may not reside in the documents tree of a web server.
    6. Pass through authentication must not allow access to the database based solely upon a remote user's authentication on the remote host.
    7. Passwords or pass phrases used to access a database must adhere to the **Password Policy**
  1. **Retrieval of Database Usernames and Passwords**
     1. If stored in a file that is not source code, then database usernames and passwords must be read from the file immediately prior to use. Immediately following database authentication, the memory containing the username and password must be released or cleared.
     2. The scope into which you may store database credentials must be physically separated from the other areas of your code, e.g., the credentials must be in a separate source file. The file that contains the credentials must contain no other code but the credentials (i.e., the username and password) and any functions, routines, or methods that will be used to access the credentials.
     3. For languages that execute from source code, the credentials' source file must not reside in the same browsable or executable file directory tree in which the executing body of code resides.
  2. **Access to Database usernames and passwords**
     1. Every program or every collection of programs implementing a single business function must have unique database credentials. Sharing of credentials between programs is not allowed.
     2. Database passwords used by programs are system-level passwords as defined by the **Password Policy**.
     3. Developer groups must have a process in place to ensure that database passwords are controlled and changed in accordance with the **Password Policy**. This process must include a method for restricting knowledge of database passwords to a need-to-know basis.

**References**

|  |
| --- |
| **Document Name** |
| Password Policy |
| Secure Coding Policy |
| Exceptions Policy |
|  |
|  |
|  |

**Outputs**

The following records need to be kept and stored securely.

|  |  |  |  |
| --- | --- | --- | --- |
| **Record** | **Responsible Person** | **Retention** | **Disposition** |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

All records must be stored in the pre-allocation location. All physical copies need to be stored in a lockable cabinet or drawer.

**Enforcement**

An employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment. A violation of this policy by a temporary worker, contractor or vendor may result in the termination of their contract or assignment with Vital College.

Any exception to the policy must comply with the **Exceptions Policy**.

**Definitions**

|  |  |
| --- | --- |
| **Terms** | **Description** |
| **LDAP server** | Lightweight Directory Access Protocol, is an Internet protocol that email, and other programs use to look up information from a server |

A black and white drawing of a handwritten note

Description automatically generated with low confidence

**DIRECTOR name** Duncan MacNicol **DIRECTOR signature**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**Signed at** Durban **on this** 20th day of February 2021



|  |  |  |
| --- | --- | --- |
|  | **Vital College (Pty) Ltd** | |
| Authorised by: | Duncan MacNicol |
| Date Authorised: | 20 February 2021 |
| Document Number: | VC-008 |

**Direct Marketing Policy**

1. **Introduction**
2. **Overview**

The purpose of this policy is to ensure Vital College markets to their clients and prospects in a way that respects their privacy, respects their interests and ensures the client or prospect has given us the necessary consent to market to them directly, thus ensuring Vital College is compliant with section 69 of the POPI act.

1. **Scope**

All employees, contractors, consultants, temporary and other workers at Vital College, including all personnel affiliated with third parties must adhere to this policy. This policy applies to clients or prospective clients of Vital College.

1. **Policy Statement**
   1. **Consent**

The processing of personal information of a data subject for the purpose of direct marketing by means of any form of electronic communication, including automatic calling machines, facsimile machines, SMSs, or e-mail is prohibited unless the data subject:

* Has given consent
* They are a client/customer, and the processing of their data is of the client’s best interest
  1. **When may Vital College approach a data subject?**

Vital College may only approach a data subject taking into account the below:

* Their consent is required
* If they have not previously withheld consent
* Vital College may only approach a data subject once
  1. **How does Vital College obtain consent?**

The subject’s consent must be requested in the following ways:

* Opt-in on Vital College website
* Manual opt-in form
* In Vital College client contracts
* In written consent either via a signed document or in email.

Each opt-in form needs to clearly state that the collection of such consent is for the purpose of direct marketing, if this is not stated, Vital College may not process this information for the use of direct marketing.

* 1. **When is processing of personal information for direct marketing purposes allowed?**

Processing the personal information of a customer or data subject is acceptable if:

* The contact details of the client was obtained when a sale of a product or service is made
* For the purpose of direct marketing similar products that is in the client’s best interest
* For the primary purpose of marketing only
* The client or data subject has not refused to receive communication or has previously opted out.
  1. **What is required in the direct marketing message?**

All direct marketing communication must contain the following:

* Details and identity of the sender (or the person on whose behalf the communication has been sent)
* An address or contact details to which the recipient may send a request to stop receiving such communication
* Optionally, an opt out button that directly links to Vital College CRM system

1. **Who should send direct marketing communication?**

It is recommended that all communication come from the marketing/sales department in order to ensure a central hub for direct marketing compliance. The marketing/sales department will also make use of best practice direct marketing systems that simplify the process of complying and to ensure every single marketing communication is aligned with section 69 of the POPI act.

1. **References**

|  |
| --- |
| **Document Name** |
| Exceptions Policy |
| Information Classification Policy |
|  |

1. **Outputs**

The following records need to be kept and stored securely.

|  |  |  |  |
| --- | --- | --- | --- |
| **Record** | **Responsible Person** | **Retention** | **Disposition** |
| Date of information collected | Marketing Manager | Until the information is no longer needed | Delete / Shred |
| Date of opt-out | Marketing Manager | 5 years | Delete |
|  |  |  |  |

All records must be stored in the pre-allocation location. All physical copies need to be stored in a lockable cabinet or drawer.

1. **Enforcement**

 An employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment. A violation of this policy by a temporary worker, contractor or vendor may result in the termination of their contract or assignment with Vital College.

Any exception to the policy must comply with the **Exceptions Policy**.

1. A black and white drawing of a handwritten note

   Description automatically generated with low confidence**Definitions**

|  |  |
| --- | --- |
| **TERMS** | **DESCRIPTION** |
| **CRM** | A customer relationship management system where all client/customer information is stored on. |

**DIRECTOR name** Duncan MacNicol **DIRECTOR signature**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**Signed at** Durban **on this** 20th day of February 2021



|  |  |  |
| --- | --- | --- |
|  | **Vital College (Pty) Ltd** | |
| Authorised by: | Duncan MacNicol |
| Date Authorised: | 20 February 2021 |
| Document Number: | VC-009 |

**Disposal and Destruction Policy**

1. **Introduction**
   1. **Overview**

Technology equipment often contains parts which cannot simply be thrown away. Proper disposal of equipment is both environmentally responsible and often required by law. In addition, hard drives, USB drives and other storage media contain various kinds of Vital College data, some of which is considered sensitive. In order to protect our data, all storage mediums must be properly erased before being disposed of. However, simply deleting or even formatting data is not considered sufficient. When deleting files or formatting a device, data is marked for deletion, but is still accessible until being overwritten by a new file. Therefore, special tools must be used to securely erase data prior to equipment disposal.

* 1. **Scope**

This policy applies to any computer/technology equipment or peripheral devices that are no longer needed within Vital College including, but not limited to the following: computers, servers, hard drives, laptops, portable storage devices (i.e., USB drives) and backup tapes and physical printed records. This policy does not apply to Solid State Drives, when files are deleted from a solid-state drive, they are permanently deleted with no chance of data recovery.

The purpose of this policy it to define the guidelines for the disposal of technology equipment and components owned by Vital College

1. **Policy Statement**
   1. **Technology Equipment Disposal**
      1. When Technology assets have reached the end of their useful life, they should be sent to the IT Team office for proper disposal.
      2. The IT Team will securely erase all storage mediums in accordance.
      3. All data including, all files and licensed software shall be removed from equipment using disk sanitizing software that cleans the media overwriting each and every disk sector of the machine with zero-filled blocks.
      4. All electronic drives must be degaussed or overwritten with a commercially available disk cleaning program. Hard drives may also be removed and rendered unreadable (drilling, crushing or other demolition methods).
      5. Technology equipment with non-functioning memory or storage technology will have the memory or storage device removed and the memory or storage will be physically destroyed.

**Destruction of records**

All Business units, branches and regions shall annually evaluate records in their possession or under their control to determine if any records are due for destruction according to this policy.

* 1. For Engagement / client records,
     1. The Destruction Register must be sent to the appropriate manager for review and confirmation of which files may be destroyed
     2. In the event that the manager is unavailable, the Product Executive (PE) or Product Manager (PM) must provide sign off for the relevant engagement and working papers files to be destroyed
     3. Any files relating to an engagement that is the subject of any litigation or possible litigation should not be destroyed until the litigation or threat thereof has passed
  2. For Business, Contracts and Company records,
     1. The Destruction Register must be sent to the appropriate manager for review and confirmation of which files may be destroyed
     2. In the event that the RM is unavailable, the PE or PM must provide sign off for the relevant engagement files to be destroyed
     3. Any files relating to an engagement that is the subject of any litigation or possible litigation should not be destroyed until the litigation or threat thereof has passed
  3. For Risk Management records,
     1. The Destruction Register must be sent to the Functional Risk Management Partner for review and confirmation of which files may be destroyed
     2. In the event that the Functional Risk Management Partner is unavailable, the National Functional Risk Management must provide sign off for the relevant files to be destroyed
     3. Any files relating that is the subject of any litigation or possible litigation should not be destroyed until the litigation or threat thereof has passed
  4. Destruction of records must be performed in a secure manner which retains an appropriate level of confidentiality during execution in accordance with the **Information Classification Policy.**
  5. Confidential records shall only be destroyed through a process that prevents the reconstruction of the contents thereof after destruction.

**Destruction Register**

A Destruction Register must be maintained and updated for all files that are destroyed as part of the annual record retention processes, the register must at least record the following information,

* 1. For Client Engagement Records
     1. engagement name/fin code
     2. description of records to be destroyed
     3. date of destruction
     4. reason for destruction
     5. engagement RM approval
  2. For Business, Contracts and Company records,
     1. description of records to be destroyed
     2. engagement name/code (if applicable)
     3. date of destruction
     4. reason for destruction
     5. appropriate Partner approval
  3. For Risk Management records,
     1. description of records to be destroyed
     2. engagement name/code (if applicable)
     3. date of destruction
     4. reason for destruction
     5. Head of department approval

The destruction register must be centrally managed by the Records Management Officer.

A Destruction Register must be produced of all client / engagement records that have reached the end of its retention period.

**References**

|  |
| --- |
| **Document Name** |
| Exceptions Policy |
| Destruction Register |
|  |
|  |
|  |
|  |

**Outputs**

The following records need to be kept and stored securely.

|  |  |  |  |
| --- | --- | --- | --- |
| **Record** | **Responsible Person** | **Retention** | **Disposition** |
| Destruction Register | Receptionist | 7 Years | Deletion/Shredding |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

All records must be stored in the pre-allocation location. All physical copies need to be stored in a lockable cabinet or drawer.

**Enforcement**

An employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment. A violation of this policy by a temporary worker, contractor or vendor may result in the termination of their contract or assignment with Vital College.

Any exception to the policy must comply with the **Exceptions Policy**.

**Definitions**

|  |  |
| --- | --- |
| **Terms** | **Description** |
|  |  |

A black and white drawing of a handwritten note

Description automatically generated with low confidence

**DIRECTOR name** Duncan MacNicol **DIRECTOR signature**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**Signed at** Durban **on this** 20th day of February 2021



|  |  |  |
| --- | --- | --- |
|  | **Vital College (Pty) Ltd** | |
| Authorised by: | Duncan MacNicol |
| Date Authorised: | 20 February 2021 |
| Document Number: | VC-010 |

**Exceptions Policy**

**Introduction**

* 1. **Overview**

The purpose of this policy is to ensure that the best interests of Vital College are maintained. All policies and procedures are to be followed for best practice and adherence to compliance requirements. Where there may be a requirement for an exception, careful consideration must be considered to maintain the best interest and reputation of Vital College and keep within the legislative and compliance requirements.

In such cases, an exception must be documented and approved using this process specified herein.

* 1. **Scope**

All employees, contractors, consultants, temporary and other workers at Vital College, including all personnel affiliated with third parties must adhere to this policy. This policy applies to all exceptions required to any policy or procedure implemented within Vital College.

1. **Policy Statement**
   1. **Exception Allowances**

An exception to a published policy, procedure, or process may be granted in any of the following situations (including IT or information security policies and procedures):

* Temporary exception, where immediate compliance would disrupt critical operations.
* Another acceptable solution with equivalent protection is available.
* A superior solution is available.
* A legacy system is being retired and compliance is not possible (risk must be managed).
* Long-term exception, where compliance would adversely impact business.
* Compliance would cause a major adverse financial impact that would not be offset by the reduced risk occasioned by compliance (i.e., the cost to comply offsets the risk of non-compliance).
  1. **Exception Application Requirements**

The exception request must document:

* Description of the exception required.
  + The nature of the non-compliance, i.e., specific deviation from the policy/standard
* The specific policy/standard for which an exception is being requested.
* Reason for the exception;
  + Why an exception is required, e.g., what business need or situation exists, what alternatives were considered, and why are they not appropriate
* Assessment of the potential risk posed by non-compliance, i.e., if the exception is granted
* Plan for managing or mitigating those risks, e.g. compensating controls, alternative approaches
* Anticipated length of non-compliance
* Additional information as needed, including any specific conditions or requirements for approval
  1. **Exception Approval Process**

All requests for exception must be signed by the person responsible for implementing the standards or controls. If the requester is not that person, then the responsible support staff must co-sign.

All requests for exception must be reviewed and approved by the relevant executive with authority for the resource for which the exception is being requested. Appropriate consideration for information security must be considered and consultation with the MINS where required.

Requests for exceptions must be submitted to the Compliance department for submission for review for validity and are not automatically approved. Once it has been minute as approved by the department, the exception is approved. Requests for exception that create significant risk to the infrastructure without compensating controls will not be approved.

Requests for exception must be periodically reviewed to ensure that assumptions or business conditions have not changed. Renewals are not automatically approved; New Request forPolicy/Procedure **Exception Form** must be completed, and the process followed again. Time should be made in advance of the expiry of the exception to allow for the approval process to be followed should there be a need to continue exception.

Enforcement procedures for non-compliance are defined in those policies and standards.

Requests for exception may be revoked in the event of a security incident or policy violation using established incident response procedures.

* 1. **Policy/Procedure Change**

If a certain type of exception is constantly being requested and approved, it may mean the relevant Policy or procedure needs to be adjusted to include the exception as a norm.

If a superior solution is available, an exception will be granted until the solution can be reviewed, and standards or procedures can be updated to allow for a better solution.

The exception process is intended to be a generic method that applies to all IT/information security policies and standards.

1. **Procedure**
   1. **Exception Application Procedure**
      1. Requester requests an exception form by contacting [Authorised by](mailto:compliance@labournet.com). The latest version of the form can be accessed on internal servers.
      2. Requester completes the form and obtains all required signatures.
      3. Requester emails the signed form to [Authorised by](mailto:compliance@labournet.com) for verification. And if satisfied, they will send on to the DIRECTOR for authorisation.
      4. The Compliance Officer will gather any necessary background information, determine if other administrative officials need to be consulted, and make a recommendation to approve or deny the request.
      5. The Compliance Officer will contact the requester if additional information is required.
      6. The request will be submitted to the Governance and Compliance Committee and will receive final approval which shall be minute in the meeting notes.
      7. The Compliance Manager will approve or deny the request for an exception and notify the requester and manager in writing as to the basis for the approval or an explanation of the denial.
      8. If approval is contingent upon meeting specific requirements not documented in the request form, the requester must sign and submit an updated request form to [Authorised by](mailto:compliance@labournet.com).
      9. Departments may appeal a denial by submitting additional information or requesting a meeting to discuss the decision. After that, all decisions will be considered final.
      10. All requests for exception will be documented and retained by the Compliance Officer.
      11. Exceptions will be valid for a maximum of one year. Duration must be specified on the request form.
      12. If the conditions have substantially changed, a new request for exception must be submitted and documented.

**References**

|  |
| --- |
| **Document Name** |
| Exception Form |
|  |
|  |
|  |
|  |
|  |

**Outputs**

The following records need to be kept and stored securely.

|  |  |  |  |
| --- | --- | --- | --- |
| **Record** | **Responsible Person** | **Retention** | **Disposition** |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

All records must be stored in the pre-allocation location. All physical copies need to be stored in a lockable cabinet or drawer.

**Enforcement**

An employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment. A violation of this policy by a temporary worker, contractor or vendor may result in the termination of their contract or assignment with Vital College.

Any exception to the policy must comply with the **Exceptions Policy**.

**Definitions**

|  |  |
| --- | --- |
| **TERMS** | **DESCRIPTION** |
| **MINS** | Manager: IT Infrastructure, Network and Security |

A black and white drawing of a handwritten note

Description automatically generated with low confidence

**DIRECTOR name** Duncan MacNicol **DIRECTOR signature**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**Signed at** Durban **on this** 20th day of February 2021



|  |  |  |
| --- | --- | --- |
|  | **Vital College (Pty) Ltd** | |
| Authorised by: | Duncan MacNicol |
| Date Authorised: | 20 February 2021 |
| Document Number: | VC-012 |

**Incidents and Non-conformance Procedure**

1. **Introduction**
2. **Overview**

The purpose of this procedure is to describe all activities related to the initiation and keeping of records of corrections and corrective actions. This procedure is applied to all activities implemented in the Information Security Management System (ISMS).

1. **Scope**

This procedure applies to all employees and activities related to the initiation, and keeping of records of corrections, as well as corrective actions.

1. **Statement**
2. **Reporting of Incidents, Non-conformance, and Improvements**

All information security incidents, non-conformance, deviations, feedback, and improvements must be loaded on the **Incidents and Improvements Form** on the internal server. Completing this form will trigger a workflow whereby the information will be stored in the internal server to be actioned by the allocated risk area. The form contains the following categories:

1. Information Security Incident
2. Interested Party Feedback
3. Change Management
4. Policy/Procedure Deviation
5. Supplier Performance
6. **Audit Findings**

Audit findings and non-conformances shall be loaded in accordance with the categories described above onto the **Incidents and Improvements Form** to be actioned by allocated risk areas.

1. **References**

|  |
| --- |
| **Document Name** |
|  |
|  |

1. **Outputs**

The following records need to be kept and stored securely.

|  |  |  |  |
| --- | --- | --- | --- |
| **Record** | **Responsible Person** | **Retention** | **Disposition** |
| Information Security Incident |  |  |  |
| Interested Party Feedback |  |  |  |
| Change Management |  |  |  |
| Policy/Procedure Deviation |  |  |  |
| Supplier Performance |  |  |  |
|  |  |  |  |

All records must be stored in the pre-allocation location. All physical copies need to be stored in a lockable cabinet or drawer.

1. **Enforcement**

An employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment. A violation of this policy by a temporary worker, contractor or vendor may result in the termination of their contract or assignment with Vital College.

Any exception to the policy must comply with the **Exceptions Policy**.

1. **Definitions**

|  |  |
| --- | --- |
| **Terms** | **Description** |
| **Non-conformity** | is any failure to meet the requirements of the standards, internal documentation, regulations, contractual and other obligations within the ISMS. |
| **Information Security Incident** | An information security incident is a suspected, attempted, successful, or imminent threat of unauthorized access, use, disclosure, breach, modification, or destruction of information; interference with information technology operations; or significant violation of policies relating to data and the protection of information |
|  |  |
|  |  |
|  |  |

A black and white drawing of a handwritten note

Description automatically generated with low confidence

**DIRECTOR name** Duncan MacNicol **DIRECTOR signature**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**Signed at** Durban **on this** 20th day of February 2021



|  |  |  |
| --- | --- | --- |
|  | **Vital College (Pty) Ltd** | |
| Authorised by: | Duncan MacNicol |
| Date Authorised: | 20 February 2021 |
| Document Number: | VC-013 |

**Information Classification Policy**

1. **Introduction**
2. **Overview**

Vital College has a moral, legal, and ethical responsibility to protect Vital College’s information assets. Along with this Vital College needs to protect proprietary and strategic information to ensure the sustainability of the organization. As an industry leader, it is critical for Vital College to set the standard for the protection of information assets from unauthorized access, compromise, or disclosure. Vital College has adopted this information classification policy as an element of its methodology to protect its information assets.

1. **Scope**

The scope of this policy extends to all information assets. The objective is to ensure that all reasonable measures have been taken to only permit access to authorized personnel. This is done through information identification and classification as to reduce the risk of accidental distribution of information as well as clarifying what information can be shared in certain situations.

1. **Policy Statement**
2. **Classification**

All Vital College personnel and associates, (including but not limited to; employees, managers, contractors, temporary staff, consultant, etc.) share the responsibility for ensuring that Vital College information assets receive the appropriate level of protection through complying with the following prescripts:

1. Information owners shall be responsible for assigning classifications to the information assets per the standard information classification table described below.
2. Where practicable, the information category shall be embedded in the information itself.
3. Information assets are to be marked with classification on the cover page as well as in the header or top right corner of any document.
4. All Vital College personnel and associates (including but not limited to; employees, managers, contractors, temporary staff, consultants, etc.) shall be guided by the information category in the Classification Table related handling of Vital College information and information assets.
5. In the case of Restricted classification, the information or document will retain the information classification of “Restricted” irrespective of the intended use or distribution thereof. The recipient of the information must sign an NDA together with an executive representative from Vital College. NDA’s must be stored on a company drive as per the **Acceptable Use Policy**.

1. **Classification Table**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
|  | **DESCRIPTION** | **SAMPLE DOCUMENTS / RECORDS** | **MARKING** | **PHYS & ADMIN CONTROLS** | **DISTRIBUTION** | **DESTRUCTION / DISPOSAL** |
| **PUBLIC - O** | Information that may be broadly distributed without causing damage to the organization, its employees, and stakeholders.  These documents may be disclosed or passed to persons outside the organization. | Marketing materials authorized for public release such as advertisements, brochures, published annual accounts, Internet Web pages, catalogues, external vacancy notices, release notices. | None / Not required | None | No restrictions | Recycling/trash in accordance with the **Disposal and Destruction Policy** |
| **CONFIDENTIAL – C** | Information whose unauthorized disclosure, particularly outside the organization, would be inappropriate and inconvenient.        Disclosure to anyone outside of Vital College requires management authorization. | Most corporate information falls into this category.    Departmental memos, information on internal bulletin boards, training materials, policies, operating procedures, work instructions, guidelines, phone and email directories, marketing, or promotional information (prior to authorized release), investment options. transaction data, productivity reports, disciplinary reports, contracts, Service Level Agreements, internal vacancy notices, intranet Web pages, Client information, ID numbers and personal information, Monthly profit and loss reports, all supplier and customer on-boarding forms. | **“CONFIDENTIAL"**    Apply to the **TOP RIGHT** corner of each page and on the Cover page | **Author:**  Responsible for proper markings and document control.    **User:**  Responsible for proper storage in accordance with the **Clean Desk Policy** | **Internal:**  If possible, hand deliver in person to the designated recipient.  Where not possible to perform such in person, use an internal mail envelope marked as “Confidential” and addressed to the recipient.    **External:** use a sealed envelope or container. Hand deliver or send by registered mail/courier to ID identified recipient only - not transferable.  **Electronic:**  Use internal email system. Encryption is required for transmission to external email addresses.  Media containing such data shall be encrypted.  **FAX:**  Requires phone confirmation of receipt of a test page immediately prior to sending the FAX, and phone confirmation of full receipt. | **Paper documents:**  Shred in accordance with the **Disposal and Destruction Policy**    **Electronic data:**  Erase or degauss magnetic media.  Send CDs, DVDs, dead hard drives, laptops, etc. in accordance with the **Disposal and Destruction Policy** |
| **RESTRICTED - R** | Highly sensitive or valuable information, both proprietary and personal.  Must not be disclosed outside of the organization without the explicit permission of an Executive or Director-level senior manager. | Passwords and PIN codes, VPN tokens, credit, and debit card numbers, other highly sensitive or valuable proprietary information, source code, Detailed Security Reports, most accounting data and all internal financial reports, Financial Statements, Audit Reports, Acquisitions and Shareholder Agreements. | **“RESTRICTED"**    Apply to the **TOP RIGHT** corner of each page and on the Cover Page. | **Originator:**  Responsible for ensuring that confidential information is distributed on a strict need-to-know basis.    **Recipient:**  Responsible for ensuring that confidential information is kept in accordance with the **Clean Desk Policy** | **Internal:**  Use a sealed envelope or container. Hand deliver to designated recipient - not transferable.  **External:** use a sealed envelope or container. Hand deliver or send by registered mail/courier to ID identified recipient only - not transferable.  **Electronic:**  Use the internal email system only. Encrypt data.  **Faxing:**  Requires phone confirmation of receipt of a test page immediately prior to sending the FAX, and phone confirmation of full receipt. | **Paper documents:**  Shred in accordance with the **Disposal and Destruction Policy.**    **Electronic data:**  Erase or degauss magnetic media.  Send CDs, DVDs, dead hard drives, laptops, etc. in accordance with the **Disposal and Destruction Policy** |

1. **References**

|  |
| --- |
| **Document Name** |
| Acceptable Use Policy |
| Disposal and Destruction Policy |
| Clean Desk Policy |
| Documented Information Policy and Procedure |
| Mutual Non-Disclosure Agreement |
|  |

1. **Outputs**

The following records need to be kept and stored securely.

|  |  |  |  |
| --- | --- | --- | --- |
| **Record** | **Responsible Person** | **Retention** | **Disposition** |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

All records must be stored in the pre-allocation location. All physical copies need to be stored in a lockable cabinet or drawer.

1. **Enforcement**

An employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment. A violation of this policy by a temporary worker, contractor or vendor may result in the termination of their contract or assignment with Vital College.

Any exception to the policy must comply with the **Exceptions Policy**.

1. **Definitions**

|  |  |
| --- | --- |
| **TERMS** | **DESCRIPTION** |
| **Business** | When referring to “Business” it is referring to the key players who can speak on behalf of the business needs. |
| **Development Team** | This term is primarily used to refer to the developers specifically. It is occasionally also used to refer to the team, who as a whole, are involved in the development lifecycle. |
| **Information Asset** | An information asset is a piece of information, such an employee record, a customer list, or a financial report, that is valuable to a company or organisation.  A piece of information that is owned by the company or organisation, eg. Vital College |
| **Information Owners** | This is the person who has compiled an information asset or a document, or manager of such a document or information asset. |
| **Vital CollegePersonnel** | Any person or entity in the employment of Vital College or provides a service to Vital College. |
| **NDA** | A non-disclosure agreement (NDA) is a legal contract between at least two parties that outlines confidential material, knowledge, or information that the parties wish to share with one another for certain purposes but wish to restrict access to or by third parties. |

A black and white drawing of a handwritten note

Description automatically generated with low confidence

**DIRECTOR name** Duncan MacNicol **DIRECTOR signature**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**Signed at** Durban **on this** 20th day of February 2021



|  |  |  |
| --- | --- | --- |
|  | **Vital College (Pty) Ltd** | |
| Authorised by: | Duncan MacNicol |
| Date Authorised: | 20 February 2021 |
| Document Number: | VC-014 |

**Information Security Incident Response Policy**

1. **Introduction** 
   1. **Overview**

This policy sets out a framework of governance and accountability for information security incidents across Vital College.

Vital College takes information security very seriously. It is necessary to take prompt action in the event of any actual or suspected breaches of information security or confidentiality to avoid the risk of harm to individuals, damage to operational business and severe financial, legal, and reputational costs to the organization.

1. **Purpose**

This policy provides a framework for reporting and managing:

* Security incidents affecting Vital College information and IT Systems
* Loss, disclosure, or corruption of information or devices
* Near misses and information security concerns

1. **Objectives**

This policy aims to support the prompt and consistent management of information security incidents in order to minimise any harm to individuals or Vital College and reduce the risk of future breaches of security.

To this end all users of Vital College information and IT systems need to:

* **report all actual or suspected information security incidents immediately on discovery to their manager and** **Authorised by.**

The policy and its supporting procedures provide a clear and consistent methodology to help to ensure that actual and suspected incidents and near misses are:

* reported promptly and escalated to the right people who can take timely and appropriate action
* recorded accurately and consistently to assist investigation and highlight any actions necessary to strengthen information security controls

Vital College will deploy lawful and proportionate measures to protect information systems by:

* monitoring logs and traffic on its IT networks and systems to detect and alert staff to cyber security attacks and system outages
* maintaining adequate logs and evidence to enable investigation of incidents and preserve the chain of custody where this information is required for legal or evidential purposes

1. **Scope**

4. 1. **What is an information security incident?**

An information security incident is any event that has the potential to affect the confidentiality, integrity or availability of Vital College information, in any format, or IT systems in which this information is held. What may appear to be a physical security or IT issue may also be an information security incident and vice-versa.

Examples of information security incidents can include but are not limited to:

* Accidental or deliberate disclosure of **HIGH** or **MEDIUM RISK** information to unauthorised individuals e.g. an email containing unencrypted high-risk personal information sent to unintended recipients
* Unauthorised sharing of **HIGH** or **MEDIUM RISK** information with an external cloud storage service or contractor
* Loss or theft of paper or electronic records, or equipment such as tablets, laptops and smartphones or other devices on which data is stored
* Inappropriate access controls allowing unauthorised use of information
* Attempts to gain unauthorised access to computer systems, e.g. hacking
* Records altered or deleted without authorisation by the data “owner”
* Introduction of malware into a computer or network, e.g. a phishing or ransomware attack
* Denial-of-service or other cyber-attack on IT systems or networks
* A power outage that affects access to IT systems and information services
* “Blagging” offence where information is obtained by deception
* Breaches of physical security e.g. forcing of doors or windows into secure room or filing cabinet containing confidential information left unlocked in accessible area
* Leaving IT equipment unattended when logged-in to a user account without locking the screen to stop others accessing information
* Audible discussion of confidential topics in public
* Covert or unauthorised recording of meetings and presentations
* In general, an Information Security Incident is any event that resulted in, or could have resulted in:
* Disclosure of confidential information to an unauthorised person.
* The integrity of the system or data being compromised.
* Embarrassment to Vital College.
* Financial loss.
* Disruption to information processing systems.

**In general, an Information Security Incident is any event that resulted in, or could have resulted in:**

* Disclosure of confidential information to an unauthorised person.
* The integrity of the system or data being compromised.
* Embarrassment to Vital College.
* Financial loss.
* Disruption to information processing systems.
  1. **This policy applies to:**
* All information created or received by Vital College in any format, whether used in the workplace, stored on portable devices and media, transported from the workplace physically or electronically or accessed remotely
* All IT systems managed by, or on behalf of Vital College
* Any other IT systems on which Vital College information is held or processed
  1. **Who is affected by this policy?**

This policy applies to all users of Vital College information.

1. **Policy**
   1. **All users who are given access to Vital College information, IT and communications facilities have a responsibility to:**
      1. Minimise the risk of vital or confidential information being lost or falling into the hands of people who do not have the right to see it.
      2. Protect the security and integrity of IT systems on which vital or confidential information is held and processed.
      3. Report suspected information security incidents promptly so that appropriate action can be taken to minimise harm.

**References**

|  |
| --- |
| **Document Name** |
|  |
|  |
|  |
|  |
|  |
|  |

**Outputs**

The following records need to be kept and stored securely.

|  |  |  |  |
| --- | --- | --- | --- |
| **Record** | **Responsible Person** | **Retention** | **Disposition** |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

All records must be stored in the pre-allocation location. All physical copies need to be stored in a lockable cabinet or drawer.

**Enforcement**

An employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment. A violation of this policy by a temporary worker, contractor or vendor may result in the termination of their contract or assignment with Vital College.

Any exception to the policy must comply with the **Exceptions Policy**.

**Definitions**

|  |  |
| --- | --- |
| **TERMS** | **DESCRIPTION** |
| **Information** | The definition of information includes, but is not confined to, paper and electronic documents and records, email, voicemail, still and moving images and sound recordings, the spoken word, data stored on computers or tapes, transmitted across networks, printed out or written on paper, carried on portable devices, sent by post, courier or fax, posted onto intranet or internet sites or communicated using social media. |
| **HIGH RISK Confidential information** | This can be summarised as:   * Any personal information that would cause damage or distress to individuals if disclosed without their consent. * Any other information that would prejudice Vital College or another party’s interests if it were disclosed without authorisation. |
| **MEDIUM RISK Confidential information** | This can be summarised as:   * Any personal information that the individuals have not agreed to share e.g., lists of staff who have not completed training * Any other information to which access must be limited on a business need to see basis e.g., a draft report |
| **Encryption** | The process of using a cipher, algorithm, or other key to convert plain text into cypher text so that it cannot be read without using another key to convert it back into plain text |

A black and white drawing of a handwritten note

Description automatically generated with low confidence

**DIRECTOR name** Duncan MacNicol **DIRECTOR signature**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**Signed at** Durban **on this** 20th day of February 2021



|  |  |  |
| --- | --- | --- |
|  | **Vital College (Pty) Ltd** | |
| Authorised by: | Duncan MacNicol |
| Date Authorised: | 20 February 2021 |
| Document Number: | VC-015 |

**Information Security Policy**

**Purpose**

The purpose of the Information Security Framework is:

* To establish an approach to information security.
* To detect and protect against the compromise of information security such as misuse of data (physical and electronic), networks, computer systems and applications.
* To protect the reputation of the company concerning its ethical and legal responsibilities.
* To observe the rights and protect the privacy of our customers.

Vital College is fully committed to ensuring the Confidentiality, Integrity and Availability of the data entrusted to us by our clients and partners.

**Information Security Policy**

Vital College recognises the disciplines of confidentiality, integrity and availability in Information Security Management are integral parts of its management function. The management of Vital College views these as primary responsibilities and fundamental to the best business practice of adopting appropriate Information Security Controls.

Vital College Information Security policy seeks to operate to the highest standards continuously and to focus on continual improvement through annual review.

We will:

* Comply with all the applicable laws, regulations, and contractual obligations.
* Implement continual improvement initiatives, including risk assessment and risk treatment strategies, while making the best use of its management resources to better Information Security requirements.
* Communicate our Information Security objectives, and its performance in achieving these objectives, throughout the organization and to interested parties.
* Adopt an Information Security Management System comprising organizational policies and procedures which provide direction and guidance on information security matters relating to employees, customers, suppliers and interested parties who come into contact with its work.
* Work closely with our customers, business partners and suppliers in seeking to establish appropriate Information Security standards.
* Adopt a forward-looking view on future business decisions, including the continual review of risk evaluation criteria, which may have an impact on Information Security.
* Train all members of staff in the needs and responsibilities of Information Security Management.
* Constantly strive to meet, and where possible exceed, our customer’s, staff, and partners expectations.

A black and white drawing of a handwritten note

Description automatically generated with low confidenceResponsibility is for upholding this policy is truly organization-wide under the guidance and with the assistance of the DIRECTOR who encourages the personal commitment of all staff to address Information Security as part of their skills.

**DIRECTOR name** Duncan MacNicol **DIRECTOR signature**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**Signed at** Durban **on this** 20th day of February 2021



|  |  |  |
| --- | --- | --- |
|  | **Vital College (Pty) Ltd** | |
| Authorised by: | Duncan MacNicol |
| Date Authorised: | 20 February 2021 |
| Document Number: | VC-016 |

**Internal Audit Procedure**

​

1. **Introduction**
2. **Overview**

The purpose of this policy is to ensure compliance with Vital College accepted standards and requirements.

1. **Scope**

The scope of this document extends to the auditing of standards, requirements and applicable legislative requirements accepted by Vital College. This document applies to all parties operating within the Vital College network environment or utilizing Information Resources. It covers all policies and procedures implemented within the Vital College environment. All staff and contractors shall comply with this policy.

1. **Statement**
2. **Audits**

Audits shall be conducted to ensure compliance with accepted standards and requirements of Vital College. These audits shall be in the following forms:

* Internal audits
* Audits shall be conducted by the Compliance Department or on behalf of the Compliance Department.
* Policies and Procedures may be selected at random for evaluation.
* Findings shall be recorded for non-compliance and may prompt full audit.
* Non conformances must be loaded on the **Incidents and Improvements Form**as per the**Incidents and Non-Conformance Procedure.**
* Gap audits
* External verification or surveillance audits.
* External certification audits.

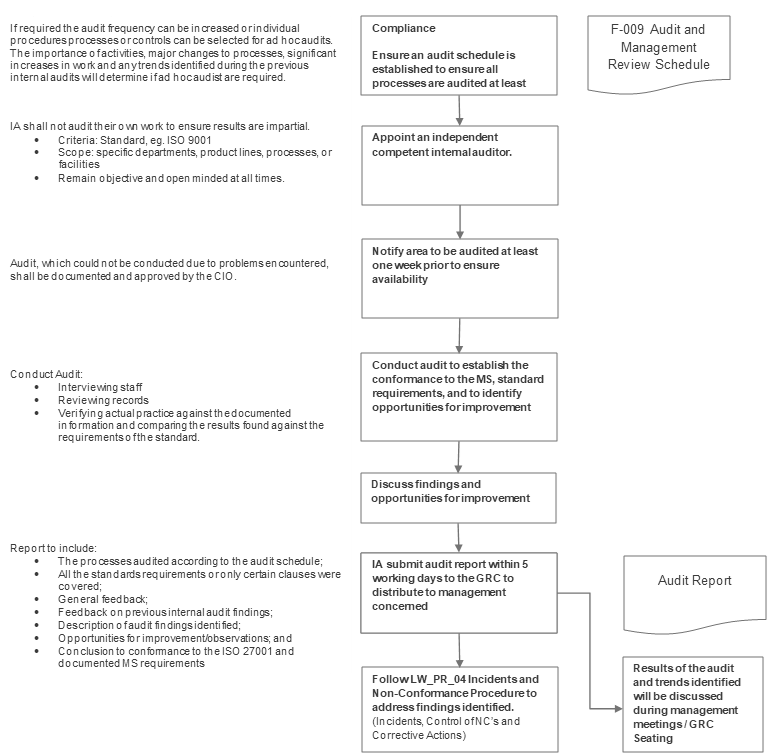
1. **Requirements**
2. External Auditors shall sign the Vital College Mutual Non-Disclosure Agreement.
3. Personnel within Vital College who conduct audits must have a non-disclosure clause in their employment contract.
4. The auditing of standards shall be conducted by nonbiased personnel aside from preliminary audits, e.g. a department may self-audit in preparation for being audited. The scheduled internal audits shall be conducted by another department or external party (Department cannot mark its own homework).
5. A report shall be compiled and distributed to the head of audited department and the head of Compliance.
6. Opportunity shall be provided for findings to be corrected and a review of the remediations shall be conducted.
7. Audits shall be scheduled in advance and agreed to by the relevant executive staff.
8. **Staff and Resources**
9. A department being audited shall make the appropriate resources and evidence available for audit.
10. Staff may refuse to send copies Information classified as non-public information, both digital and physical. However, staff shall be required to present relevant evidence or documents to auditors as requested within the duration of audit process.

1. **Process**
2. **Process Inputs and Reference Documents**

* Previous audit reports
* Control results
* Changes in the organisation
* Statutory & Regulatory requirements
* MS (Management system)
* Other Requirements

1. **Process Steps**

* Operational Audits: critical reviews of operating processes and procedures, and internal controls that mitigate area-specific risks, the effective and efficient use of resources to fulfill Vital College mission and objectives.
* Compliance Audits – Verify processes and controls used to ensure compliance with legal and regulatory requirements.
* Financial Audits - Review accounting and financial transactions to determine if commitments, authorizations, and receipt and disbursement of funds are properly and accurately recorded and reported.
* Investigative Audits - To determine irregularities, assist in determining the amount of loss, and recommending corrective measures to prevent subsequent reoccurrence.
* Technology Audits – control reviews of disaster recovery plans, system back-up procedures, and general security of data and of the physical premises to evaluate the accuracy, effectiveness, and efficiency of the Company’s electronic and information processing systems.
* See below flow diagram for the process of handling non-conformances or improvements.

****

1. **References**

|  |
| --- |
| **Document Name** |
| Incidents and Non-Conformance Procedure |
|  |
|  |
|  |
|  |
|  |

1. **Outputs**

The following records need to be kept and stored securely.

|  |  |  |  |
| --- | --- | --- | --- |
| **Record** | **Responsible Person** | **Retention** | **Disposition** |
| Incident / Improvement Report | Risk Owners (Executive) | 2 Years | Destroy |
| Audit & Management Review Schedule | Compliance | 2 Years | Destroy |
| Internal Audit Report | Auditor | 2 Years | Destroy |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

All records must be stored in the pre-allocation location. All physical copies need to be stored in a lockable cabinet or drawer.

1. **Enforcement**

An employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment. A violation of this policy by a temporary worker, contractor or vendor may result in the termination of their contract or assignment with Vital College.

Any exception to the policy must comply with the **Exceptions Policy**.

1. **Definitions**

|  |  |
| --- | --- |
| **Terms** | **Description** |
| **IA** | Internal Auditor |
| **CGRQAM** | Corporate Governance, Risk, and Quality Assurance Manager |

A black and white drawing of a handwritten note

Description automatically generated with low confidence

**DIRECTOR name** Duncan MacNicol **DIRECTOR signature**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**Signed at** Durban **on this** 20th day of February 2021



|  |  |  |
| --- | --- | --- |
|  | **Vital College (Pty) Ltd** | |
| Authorised by: | Duncan MacNicol |
| Date Authorised: | 20 February 2021 |
| Document Number: | VC-018 |

**Minimum access Policy**

**1. Introduction**

**1.1. Overview**

The purpose of this policy is to define rules and requirements for connecting to Vital College network from any host that is not managed or owned by Vital College. These rules and requirements are designed to minimize the potential exposure to Vital College from damages which may result from unauthorized use of Vital College resources. Damages include the loss of sensitive or company confidential data, intellectual property, damage to public image, damage to critical Vital College internal systems, and fines or other financial liabilities incurred as a result of those losses.

**1.2. Scope**

This policy applies to all parties operating within the Vital College network environment or utilizing Information Resources.  It covers personal computers (stand-alone or network-enabled), located at Vital College offices and Vital College production related locations, where these systems are under the jurisdiction and/or ownership of the Vital College or subsidiaries, and any personal computers, laptops, mobile device and or servers authorized to access the Vital College data networks.

1. **Policy Statement**
2. **General requirements**

It is the responsibility of Vital College employees, contractors, vendors and agents with access privileges to Vital College corporate network to ensure that their personal computer, laptop, mobile device or server conforms with the standards set out in this policy.When accessing the Vital College network from a personal computer, Authorized Users are responsible for preventing access to any Vital College computer resources or data by non-Authorized Users.  Performance of illegal activities through the Vital College network by any user (Authorized or otherwise) is prohibited. The Authorized User bears responsibility for and consequences of misuse of the Authorized User’s access.  For further information and definitions, see the **Acceptable Use Policy**.

Authorized Users will not use Vital College networks to access the Internet for outside business interests.

1. **Operational Procedures**

Before any personal computer, laptop, mobile device or server is connected to any Vital College resource it is the responsibility of the owner of such equipment to request Internal IT to assess the device before it is connected to any Vital College owned corporate network or any network managed by the Internal IT department or subsidiaries.

Internal IT will assess the personal computer, laptop, mobile device or server prior to connecting the device to the corporate network, the assessment will include all the requirements set out in section 2.3 Minimum Requirements.

1. **Minimum Requirements**
2. All Windows critical and security updated will be installed and up to date, if any pending updates are found on the device, the device will need to be updated prior to connecting to the corporate network.
3. Anti-Virus software must be installed and must be up to date. If no Antivirus is present an IT representative will install a free or trial version of Anti-Virus software to ensure the device does not contain any malicious applications or files.
4. Require employees to allow the organization to install mobile device management software, if desired by the organization, and prohibit them from taking any actions to circumvent security protections put in place by the organization.
5. Require employees who are participating in the **Minimum Access Policy** to acknowledge that they have read and agreed to the **Minimum Access Policy**.
6. Prohibit employees from utilizing any of the following applications:
7. Proxy Applications
8. Peer to Peer file transfer applications
9. File Transfer Software other than those identified by the IT department.
10. Network Monitoring software unless approved IT
11. Require employees to segregate personally owned data from company-owned data to the fullest extent possible.
12. The owner of the device will be responsible for backing up personally owned data on the device to prevent it from being lost in the event the device is wiped.
13. The Owner assumes liability for any damages caused by malfunction, viruses, etc.
14. Only authorised individuals will be given access to confidential and/or personal information based on whether the individual requires access to the confidential and/or personal information to perform their duties.
15. **References**

|  |
| --- |
| **Document Name** |
| Acceptable Use Policy |
| Minimum Access Policy |
| Exceptions Policy |
|  |
|  |
|  |

1. **Outputs**

The following records need to be kept and stored securely.

|  |  |  |  |
| --- | --- | --- | --- |
| **Record** | **Responsible Person** | **Retention** | **Disposition** |
| Scan Results | IT Manager | 12 Months | Deletion |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

All records must be stored in the pre-allocation location. All physical copies need to be stored in a lockable cabinet or drawer.

1. **Enforcement**

An employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment. A violation of this policy by a temporary worker, contractor or vendor may result in the termination of their contract or assignment with Vital College.

Any exception to the policy must comply with the **Exceptions Policy**.

1. A black and white drawing of a handwritten note

   Description automatically generated with low confidence**Definitions**

|  |  |
| --- | --- |
| **TERMS** | **DESCRIPTION** |
| **MINS** | Manager: Infrastructure, Network and Security |

**DIRECTOR name** Duncan MacNicol **DIRECTOR signature**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**Signed at** Durban **on this** 20th day of February 2021



|  |  |  |
| --- | --- | --- |
|  | **Vital College (Pty) Ltd** | |
| Authorised by: | Duncan MacNicol |
| Date Authorised: | 20 February 2021 |
| Document Number: | VC-019 |

**Entered into between:**

**Vital College**

43 Sea Cow Lake Road, Springfield, Durban,4001

And

**Insert vendor/partner Name**

Insert Reg number

*Insert vendor/partner address*

1. **Definitions**

In this Agreement, unless clearly inconsistent with or otherwise indicated by the context:

1. “the / this Agreement” means the Agreement as set out in this document and any written agreed amendments hereto.

1. “Parties” means the companies / entities and / or their respective holding companies and detailed on the front page of this Agreement, collectively.

1. “Party” means any one of the Parties as the context may indicate.

1. “Recipient” means any Party to this agreement in any manner receiving or becoming posed of the Confidential Information.

1. “Business Purpose” means any or all the following:

1. the technical integration and / or interfacing of the software products as supplied by either Party;

1. the transferring of electronic data and information between the Parties software applications;

1. the proposed internal use, by either of the Parties, of the products and / services as provided by each Party;

1. the analysis, investigation and research of each Party’s products and / or services, other than those related to the software products and / or services, and which are owned by their respective holding companies or companies owned by their holding companies, for the purposes of establishing a potential sales, service and support arrangement of these products and services, between the Parties;

1. the sharing of information regarding either parties’ current or future business or product related strategies, irrespective of such information being shared between each other verbally, or visually or in printed form.

1. “Confidential Information” means the following:

1. Intellectual property, concepts, manuals, applications, methods, technical, trade, commercial, financial and other information;

1. information in respect of knowhow, statistics, processes, financial arrangements, systems, business methods and techniques used by the company in the conduct of its business;

1. any information contained in any business or other model;

1. computer software, software concepts, specifications and internal control systems of the company;

1. trade secrets, user, consumer, research and development data, profiles, formulas and formulations;

1. all information belonging to or in the possession of the company and used by it in its business operations, including joint ventures and subsidiaries;

1. knowledge of details and particulars in regard to the company's suppliers, customers and business associates;

1. the company's methods of conducting business;

1. pricing, customer lists, customer orders, quotations, and customer requirements; and

1. any other information which relates to the business of the company which is not readily available in the ordinary and normal course of business to any competitors of the company, and which may come to the knowledge of the recipient (whether or not such information is recorded and/or transmitted orally, electronically, or in writing, whether furnished before or after the date hereof, and regardless of the manner in which it is furnished).

1. “Date of Signature” means the date upon which this Agreement is signed by the Party doing so last in time;

1. “Disclosing Party” means any of the Parties to this agreement that has disclosed or in any other manner made available, the Confidential Information as defined in this agreement, to the Recipient.

1. “Client/s” means those end users and / or customers / clients who use the software applications, services and/or products provided by the Parties.

1. “Intellectual Property” means all copyright, rights in business names, trademarks, trade names, service marks, patents, designs and/or inventions as well as all rights to source codes, trade secrets, know-how and all other rights of a similar character (regardless of whether such rights are registered and/or capable of registration) and all applications and rights to apply for protection of any of the same.
2. **Duration**

This Agreement shall commence on the Date of Signature and shall remain in force indefinitely, unless specifically cancelled by way of written agreement between the Parties.

1. **Non-Disclosure and Return of Confidential Information**
2. The Confidential Information is proprietary to the Disclosing Party and constitutes part of the assets of the business of the Disclosing Party. In order to protect the proprietary interests of the Disclosing Party in and with regard to the Confidential Information, the Recipient has agreed to the confidentiality undertakings set out herein.

1. The Recipient undertakes to procure that its employees, independent subcontractors, agents, and representatives (if any) to whom any such Confidential Information or any part thereof has been or will be disclosed, shall sign a confidentiality and non-disclosure agreement on substantially the same terms and conditions as those set out herein. Irrespective of whether these parties sign such an agreement, they shall nonetheless be considered bound by the undertakings herein.

1. The Recipient shall not disclose the Confidential Information to any person, save its Clients, authorised representatives of its Clients, employees, agents, consultants, or contractors involved in the Business Purpose and who have a need to know the Confidential Information for such Business Purpose.

1. In particular, the Recipient undertakes in favour of the Disclosing Party –

1. that it will not, without the prior written consent of the Disclosing Party, directly or indirectly –

1. use, divulge, discuss, disclose or reveal any of the Confidential Information, other than for the specified purpose;

1. divulge, discuss, disclose or reveal the Confidential Information to any person other than its employees and advisors who are required, in the course of their duties, to receive and consider the same for the specified purpose;

1. that it will procure that its directors, shareholders, employees, and advisors to whom the Confidential Information is disclosed, are informed of the confidential nature of the Confidential Information. The Recipient shall be responsible for any breach of this confidentiality undertaking by its directors, shareholders, employees and/or advisors;

1. that it will return to the Disclosing Party (promptly and at any time pursuant to a demand therefore by the Disclosing Party) any software, programs, documents, diagrams, notes, memoranda or any other records relating to the Confidential Information (irrespective of what media the same is stored in), which the Recipient has in its possession or under its control, and shall not retain any copies or précis thereof or extracts therefrom, in any form whatsoever. The Recipient further undertakes to delete and remove the Confidential Information from its electronic data bases and deliver to the Disclosing Party a certificate from any authorized director of the Recipient that it has done so.

1. The Confidential Information is acknowledged by the Recipient to be the property of the Disclosing Party and that the disclosure of the Confidential Information to the Recipient shall not be deemed to confer any right to the Confidential Information on the Recipient.

1. The obligations pursuant to this agreement shall not apply to any Confidential Information that

1. is in the possession of the Recipient prior to receipt from the Disclosing Party;

1. is or become publicly known, but only where this public knowledge is not in any manner, whether directly or indirectly, linked to or occurred as a consequence of a breach of this agreement;

1. is *bona fide* received from a third party without similar restrictions and without breach of this agreement;

1. is required to be disclosed in response to a valid order of court or other governmental agency or if disclosure thereof is otherwise required by law;

1. is independently developed by the Recipient.

1. If the Recipient is legally obliged to divulge the Confidential Information it shall, provided that circumstances permit the time to do so, forthwith and before releasing the Confidential Information, inform the Disclosing Party of the obligation.

1. The Recipient warrants that it will at all times, and in every respect, reasonably comply with the provisions of the Protection of Personal Information Act 4 of 2013 (“POPI”), including the Privacy and Data Protection Conditions contained therein. The Recipient shall be obliged to fully acquaint itself with these provisions.

1. The Recipient agrees to indemnify the Disclosing Party in any and all circumstances, against any costs, claims, proceedings, liabilities or expenses resulting from claims made against the Disclosing Party by any third party, arising out of any unauthorised disclosure or use of Confidential Information, breach of its obligations under this agreement, or breach of the provisions of POPI.

1. Save for compliance by a Party with the requirements of the JSE Securities Exchange and the Securities Regulation Panel, no Party may publish any announcement relating to the Business Purpose without the prior written consent of the other Party.

1. The Recipient agrees to protect the Confidential Information of the Disclosing Party using not less than the same standard of care that would be applied to its own proprietary, secret, or confidential information and that the Confidential Information shall be stored and disclosed in such a way as to prevent any unauthorised disclosure.

1. Nothing set out in this Agreement shall be regarded as an undertaking by either Party to conclude any agreement with the other Party or any third party.
2. **Limitation / Breach**
3. Should the Recipient breach any provision of this agreement and fail to remedy such breach within 5 (five) working days after receiving written notice from the Disclosing Party requiring it to do so, then the Disclosing Party shall be entitled, without prejudice to the Disclosing Party's other rights in law, to claim from the Recipient such damages to which it may be entitled at common law or in equity including *inter alia* specific performance. This may also include interdict proceedings in any competent Court.

1. Notwithstanding anything to the contrary contained in this agreement, neither Party shall be entitled to cancel this agreement in any circumstances whatsoever, unless both parties agree in writing to such cancellation.

1. The Recipientshall however not be liable to the Disclosing Party for indirect or special damages, howsoever arising, whether or not caused by its employees, agents and / or contractors, and regardless of form or cause of action. The provisions of this clause are also stipulated for the benefit of the employees, agents and / or contractors of the Recipient.

1. The Recipient shall further incur no liability unless court proceedings are instituted by the Disclosing Party within 1 (one) year of the cause of action arising.
2. **Domicilium and Notices**
3. The Parties choose their respective domicilium addresses for all purposes hereunder to be the addresses as detailed on the front page of this Agreement.

1. Any Party shall be entitled from time to time, by written notice to the other(s), to vary its domicilium address to any other address within the Republic of South Africa which is not a post office box or poste restante.

1. All notices given in terms of this Agreement shall be in writing and any notice given by any Party to another ("the addressee") which –

1. is delivered by hand or transmitted by e-mail or telefacsimile, shall be deemed to have been received by the addressee on the same Business Day as the date of delivery or transmission, as the case may be;

1. is posted by pre-paid registered post from an address within the Republic of South Africa to the addressee at its domicilium address for the time being shall be deemed to have been received by the addressee on the 10th (tenth) Business Day after the date of such posting.
2. **General**
3. This Agreement constitutes the entire agreement between the Parties with regard to the subject matter hereof.

1. The terms and conditions contained on any purchase order, order acceptance forms and / or invoices generated by any of the Parties, shall not apply to, supplement, or supersede any provisions of this Agreement.

1. No alteration or variation to, or consensual cancellation of this Agreement shall be of any force or effect, unless it is recorded in writing and signed by all the Parties.

1. Nothing in this Agreement constitutes either Party as the agent, principal, representative or partner of the other, and no Party shall be entitled to hold out to any third party that the relationship between the Parties is that of a partnership, joint venture, or the like.

1. No failure or delay by a Party to enforce any provision of this Agreement shall constitute a waiver or suspension of such provision or affect in any way a Party’s right to require performance of any such provision at any time in the future, nor shall the waiver of any right arising from any subsequent breach nullify the effectiveness of the provision itself.

1. No Party may cede its rights and / or delegate its obligations under this Agreement without the prior written consent of the other Party.

1. In the event that any of the terms of this Agreement are found to be invalid, unlawful or unenforceable, such terms will be severable from the remaining provisions, which shall remain of full force and effect. If any invalid term is capable of amendment to render it valid, the Parties agree to negotiate in good faith an amendment to remove the invalidity.

1. If any conflict arises in respect of the provisions contained in this Agreement and any annexure attached hereto, the provisions contained in this Agreement shall take precedence.

1. Unless otherwise agreed in writing between the Parties, no Party shall for the duration of this Agreement and for a period of 12 (twelve) months after expiry or termination thereof for its own benefit or as a representative of or agent for any third party, persuade, induce, encourage, procure, or solicit (or procure such persuasion, inducement, encouragement, procurement, or solicitation of) the personnel of the other Party:

1. to become employed, or interested, directly or indirectly in any manner whatsoever, by it or in any business which is in competition with the business carried on by the other Party; or

1. to terminate his / her employment with the other Party; or

1. to disclose any Intellectual Property of the other Party to any person not authorised by the owner of the Intellectual Property to receive it.

1. This Agreement may be signed in two or more counterparts, one or more of which may be delivered via telefax or e-mail, and the signed counterparts, taken together, shall constitute a binding agreement between the Parties.

1. Each Party acknowledges that it does not enter into this Agreement on the basis of and does not rely on any representation, warranty or other provision, whether express or implied, except as expressly provided in this Agreement. All conditions, warranties or other terms implied by statute or common law are excluded to the fullest extent permitted by the law of the Republic of South Africa.

1. Each Party warrants that it is acting as principal and not as agent for any other person, whether disclosed or otherwise.

1. This Agreement shall be governed by, construed, and interpreted in accordance with the laws of the Republic of South Africa and the Parties hereby submit and consent to the exclusive jurisdiction of the High Court of the Republic of South Africa for all purposes hereunder.

1. The Parties shall each pay their own costs of negotiating, drafting, preparing, and implementing this Agreement and any annexure to it.

1. **Data Protection**
2. By either Party submitting any personal information to the other, the disclosing Party unconditionally and voluntarily, consents to the processing of the submitted personal information for any and all purposes related to this agreement.

1. The Parties agrees and consent that its personal information may be processed by, or on behalf of either of the Parties for the purposes set out in the Agreement.

1. The Parties shall at all times comply with its obligations and procure that each of its Affiliates comply with their obligations under POPI.
2. The Parties shall ensure that any personal information that is processed by it in the course of performing its obligations under the Agreement is done in accordance with POPI.
3. Each Party shall not process, disclose, or use personal information except:
4. to the extent necessary for the provision of Services and/or Products under the Agreement; or
5. to fulfil their own obligations under the Agreement; or
6. as otherwise expressly authorised by the other Party in writing.
7. Each Party shall not disclose any personal information to any Third Party without the other Party’s prior written consent in each instance, other than to the extent required by any Regulatoror Law.
8. In the event the other Party providing such consent necessary for the disclosure of personal information to a Third Party, each Party shall:
9. make such disclosure in compliance with POPI; and
10. enter into a written agreement with the applicable Third-Party recipient of such personal information that requires such Third Party to safeguard the personal information in a manner no less restrictive than each Party’s obligations under these terms.
11. The Parties shall implement and maintain an effective security safeguards that includes, but is not limited to administrative, technical, and physical safeguards, and appropriate technical and organisational measures, in each case, adequate to insure the security and confidentiality of personal information, and to protect against any anticipated risks to the security or integrity of personal information, protect against unauthorized access to or use of personal information,protect personal information against unlawful processing or processing otherwise than in accordance with this agreement, and protect against accidental loss, destruction, damage, alteration or disclosure of personal information.
12. Without limiting the foregoing, such safeguards and measures shall be appropriate to protect against the harm that may result from unauthorised or unlawful processing, use or disclosure, or accidental loss, destruction, or damage to or of Personal Information and the nature of the personal information, and shall maintain all safeguard measures as is required by POPI.
13. Each Party shall not use, process, store, transfer or permit access to any personal information across the borders of South Africa, without the written consent of the other Party.
14. In the event of any actual, suspected, or alleged security breach, including, but not limited to, loss, damage, destruction, theft, unauthorized use, access to or disclosure of any personal information, each Party shall:
15. notify the other Party as soon as practicable after becoming aware of such event;
16. provide the other Party will all information regarding the breach in the Party’s knowledge and possession to allow the Party to ascertain what has occurred and which personal information has been affected;
17. promptly take whatever action is necessary, at each Party’s own expense, to minimise the impact of such event and prevent such event from recurring.
18. **Interpretation**
19. In this Agreement, unless the context requires otherwise :

1. words importing any one gender shall include the other two genders;

1. the singular shall include the plural and *vice versa*;

1. a reference to natural persons shall include created entities (incorporated or unincorporated) and *vice versa*;

1. “Business Day” means any day other than a Saturday, Sunday or any official public holiday within the Republic of South Africa;

1. any reference to an enactment is to that enactment as at the Date of Signature, as amended or re-enacted from time to time;

1. if any provision in a definition is a substantive provision conferring rights or imposing obligations on any Party, effect shall be given to it as if it were a substantive provision in the body of this Agreement, notwithstanding that it is only in the definition clause;

1. when any number of days (whether Business Days or calendar days) is prescribed in this Agreement, that number of days shall be reckoned exclusively of the first and inclusively of the last day, unless the last day (in the case of calendar days) falls on a Saturday, Sunday or official public holiday in the Republic of South Africa, in which event the last day shall be the next succeeding Business Day;

1. when any number of days is prescribed and it is not specified whether those days are Business Days or calendar days, they shall be deemed to be calendar days; and

1. expressions or words defined in this Agreement shall bear the same meaning in the annexures to this Agreement which do not themselves contain definitions for such expressions or words.

1. The headings in this Agreement have been inserted for convenience only and shall not be used for nor assist or affect its interpretation.

1. Words and expressions defined in any sub-clause shall, for the purposes of the clause of which that sub-clause form’s part, bear the meaning assigned to such words and expressions in that sub-clause.

**Company Rep name**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ **Company Rep signature**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**Signed at** \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**on this** \_\_\_\_\_\_\_\_ **day of** \_\_\_\_\_\_\_\_\_\_\_**20**\_\_\_

 FOR AND ON BEHALF OF **Vital College**who by signature hereof warrants his authority to so sign.

**Partner name**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ **Partner signature**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**Signed at** \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**on this** \_\_\_\_\_\_\_\_ **day of** \_\_\_\_\_\_\_\_\_\_\_**20**\_\_\_

FOR AND ON BEHALF OF**The Client / Partner**who by signature hereof warrants his authority to so sign.



|  |  |  |
| --- | --- | --- |
|  | **Vital College (Pty) Ltd** | |
| Authorised by: | Duncan MacNicol |
| Date Authorised: | 20 February 2021 |
| Document Number: | VC-020 |

**Password Policy**

1. **Introduction**
2. **Overview**

Passwords are an important aspect of computer security. A poorly chosen password may result in unauthorized access and/or exploitation of Vital College resources. All users, including contractors and vendors with access to Vital College systems, are responsible for taking the appropriate steps, as outlined below, to select and secure their passwords.

1. **Scope**

All employees, contractors, consultants, temporary and other workers at Vital College, including all personnel affiliated with third parties must adhere to this policy. This policy applies to information assets owned or leased by Vital College, or to devices or services that connect to a Vital College network or reside at a Vital College site.

1. **Policy Statement**
2. **Password Creation**
3. All user-level and system-level passwords must conform to the “Password Construction Guidelines” set out in clause 2.5 of this document.
4. Users should not use the same password for Vital College accounts as for other personal or other access (for example, personal ISP account, Internet Banking, social media accounts, etc).
5. Where possible, users should not re-use the same password for various Vital College access needs.

1. **Password Change**
2. All user-level passwords must be changed at least every sixty calendar days.
3. Password cracking or guessing may be performed on a periodic or random basis by the Vital College IT Team or Vital College security team or its delegates. If a password is guessed or cracked during one of these scans, the user will be required to change it to comply with this policy.

1. **Password Protection**
2. Refrain from sending plaintext passwords over networks or email, it could compromise security. Passwords sent in plain text can be read by anyone.
3. Passwords must not be shared with anyone. All passwords are to be treated as restricted Vital College information.
4. Passwords may be inserted into email messages, Alliance cases or other forms of electronic communication, but must be encrypted and the encryption key must be shared via a different media source. Refer to the Acceptable Encryption Policy.
5. Do not reveal a password on questionnaires or security forms.
6. Do not hint at the format of a password (for example, "my family name").
7. Do not share Vital College passwords with anyone, including administrative assistants, secretaries, managers, co-workers, and family members.
8. Do not write passwords down and store them anywhere in your workspace.
9. Do not store passwords in a file on a computer system or mobile devices (phone, tablet)
10. Do not use the "Remember Password" feature of applications (for example, web browsers).
11. Any user suspecting that his/her password may have been compromised must report the incident to the Vital College IT department immediately and request a change of passwords on all user access accounts.
12. Password managers can be used, users must refer to the pre-authorized software list, held by InfoSec and IT departments.

1. **Application Development**

Application developers must ensure that their programs contain the following security precautions:

1. Applications must support the authentication of individual users.
2. Applications that authenticate against Active directory must authenticate against a dedicated Active Directory security group.
3. Applications must not store passwords in clear text or in any easily reversible form.
4. Applications must not transmit passwords in clear text over the network.
5. Applications must provide for some sort of role management, such that one user can take over the functions of another without having to know the other's password.

1. **Password Construction Guidelines**

Passphrases are not the same as passwords. A passphrase is a longer version of a password and is, therefore, more secure. A passphrase is typically composed of multiple words. Because of this, a passphrase is more secure against "dictionary attacks".

A good passphrase is relatively long and contains a combination of upper and lowercase letters, numeric and punctuation characters.

Passwords that are listed in the password blacklist will not be available for use.

Vital College Passwords must meet three of the four characteristics below:

* Contain at least 12 alphanumeric characters.
* Contain both upper- and lower-case letters.
* Contain at least one number (for example, 0-9).
* Contain at least one special character (for example, !$%^&\*()\_+|~-­‐=\`{}[]:";'<>?,/).

1. **Password Examples**

BAD Examples

* A password containing a single dictionary word (for example, Password).
* Contains personal information (for Example, Birth Date, Birth Year, Family Names, Pet Names).
* Contain work-related information such as building names, system commands, sites, companies, hardware, or software.
* Contain number patterns such as aaabbb, qwerty, zyxwvuts, or 123321.
* Contain a common word spelled backwards, preceded, or followed by a number (for example, terces, secret1 or 1secret).
* Some variation of “Welcome123” “Password123” “Changeme123”.

1. **Administrator Enforced Policies**

All Vital College systems administrators are responsible for ensuring that the network environment and all Operating Systems within the Vital College network are configured to support this password policy. The following configuration settings must be applied to all Active Directory Forests, Active Directory Domains, Windows member servers and Non‐Windows servers which operate within any of the Vital College owned networks.

1. Enforce Password History – This must be set to 10 passwords remembered, i.e.: The user may not be able to use his/her previous 10 passwords.
2. Maximum Password Age – This must be set to 60 calendar days, so that the system enforces the change of the user’s password every 60 calendar days.
3. Minimum Password Age – This must be set to 10 calendar days, so that users can only change their passwords at will every 10 calendar days.
4. Minimum Password Length – This must be set to 12 characters.
5. Password Complexity – Must be enabled to ensure that passwords are case sensitive, alpha-numeric and contain special characters.
6. Account Lockout Duration – Lockout duration should be set to 30 minutes.
7. Account Lockout Threshold – Lockout Threshold should be set to 5 bad consecutive password attempts.
8. Reset Account Lockout Counter – Reset Account Lockout Counter should be set to 30 minutes.
9. IT Administrators need to update the password blacklist annually. The blacklist needs to be recorded, approved, and communicated by the IT manager.

1. **Superuser / Administrator Passwords**

A Super User / Administrator account is a highly sensitive account and extreme caution should be taken when dealing with these accounts.

1. Superuser or Administrator passwords should never be shared with anyone inside or outside the organization.
2. All Administrators will be issued with a named Administrator account. Named administrator accounts will reflect the name of the person responsible for that specific account. The user will be responsible for their Administrator account and the safekeeping of the account password.
3. All Administrators will be held responsible for the activities on their set account.
4. All Administrator accounts must be enrolled, if supported by the system, with MFA Multi-Factor Authentication, the preference of the MFA options is, in order:
5. Authentication App
6. Phone Call
7. Alternate Email address
8. SMS

1. **Default Administrator Passwords**
2. The default Administrator account usernames must be changed, where possible.
3. The default Administrator account password must be changed during the implementation of the system.
4. The passwords for the default administrator account should only be accessible to authorized personnel.
5. Passwords for Default Administrator accounts will be changed annually and must be documented within the Access control framework document and stored in a secure location, this document should not be saved on any system within the Vital College network.
6. Passwords for default Administrator accounts should comply with the below rules, where applicable:
7. Minimum Password Length – This must be set to 20 characters.
8. Password Complexity – Must be enabled to ensure that passwords are  case sensitive, alpha-numeric and contain special characters.

1. **Local Administrator Passwords**

The "Local Administrator Password Solution" (LAPS) provides the management of local account passwords of domain-joined computers. Passwords are stored in Active Directory and protected by ACL, so only eligible users can read it or request its reset.

1. Users who are eligible to read the local administrator passwords are responsible for the safekeeping of the passwords.
2. Local Administrator passwords must not be shared with any unauthorized person.
3. Local Administrator passwords must be changed every 90 days.
4. LAPS must be enrolled on all domain-joined devices.

1. **Mobile Phone Passwords**

Mobile phones that are used to access company information must comply with the Minimum Access Policy and must have a password set and must comply with the below:

1. Minimum Password Length – This must be set to 5 characters.
2. Password Complexity – Complex numeric, repeated, or consecutive numbers, such as "1111" or "1234", aren't allowed.
3. Maximum minutes of inactivity before a password is required – 5 minutes.

1. **Password Managers**

The use of password managers has become more common, and the use of password managers is accepted within the environment, but must comply with the following:

1. Password Managers need to be enrolled with your company-issued email address.
2. Storing company passwords on a Password Managers enrolled with a personal email address is strictly prohibited.
3. Multi-factor authentication must be enabled on the account.
4. These accounts should never be shared with other internal or external parties.
5. Individual Passwords may be shared through the Password Manager application and must be controlled through the Password Manager Application.
6. Shared Passwords must be reviewed on a regular basis.
7. The use of a password generator is allowed, but the password must meet the password requirements specified in section 2.5 of this document.

1. **References**

|  |
| --- |
| **Document Name** |
| Exceptions Policy |
| Information Classification Policy |
|  |
|  |
|  |
|  |

1. **Outputs**

The following records need to be kept and stored securely.

|  |  |  |  |
| --- | --- | --- | --- |
| **Record** | **Responsible Person** | **Retention** | **Disposition** |
| Password Document | IT Manager | 5 Years | Delete / Shred |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

All records must be stored in the pre-allocation location. All physical copies need to be stored in a lockable cabinet or drawer.

1. **Enforcement**

 An employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment. A violation of this policy by a temporary worker, contractor or vendor may result in the termination of their contract or assignment with Vital College.

Any exception to the policy must comply with the **Exceptions Policy**.

1. **Definitions**

|  |  |
| --- | --- |
| **TERMS** | **DESCRIPTION** |
| **Dictionary attacks** | An attempt to gain illicit access to a computer system by using a very large set of words to generate potential passwords. |
| **Local Administrator Password Solution (LAPS)** | For environments in which users are required to log on to computers without domain credentials, password management can become a complex issue. Such environments greatly increase the risk of a Pass-the-Hash (PtH) credential replay attack. The Local Administrator Password Solution (LAPS) provides a solution to this issue of using a common local account with an identical password on every computer in a domain. LAPS resolves this issue by setting a different, random password for the common local administrator account on every computer in the domain. Domain administrators using the solution can determine which users, such as helpdesk administrators, are authorized to read passwords. |
| **Superuser / Administrator** | A user of a computer system with special privileges needed to administer and maintain the system |

A black and white drawing of a handwritten note

Description automatically generated with low confidence

**DIRECTOR name** Duncan MacNicol **DIRECTOR signature**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**Signed at** Durban **on this** 20th day of February 2021

|  |  |  |
| --- | --- | --- |
| C:\Users\JReddy\AppData\Local\Microsoft\Windows\INetCache\Content.Word\Vital small simple.jpg | **Vital College (Pty) Ltd** | |
| Authorised by: | Duncan MacNicol |
| Date Authorised: | 20 February 2021 |
| Document Number: | VC-021 |

**Physical Security Policy**

1. **Introduction**
2. **Overview**

The purpose of this document is to define rules for protection from fraud, vandalism, sabotage, accidents, and theft of information continue to increase costs for the Vital College since the co-mingling of mobility and use of personal devices continues to grow.

This Physical Security document identifies how to protect Vital College resources from unauthorized physical access and the risks associated with environmental threats and hazards.

1. **Scope**

This document is applied to all Management, staff, and contractors.

This document is applied to the entire Information Security Management System (ISMS) scope.

All IT Resources, regardless of their physical location, are used to store, process, and/or transmit Vital College electronic information in any form. This includes, but is not limited to networks, computer hardware, mobile devices, software, applications, and associated information used in the support of Vital College business.

1. **Policy**
2. **Physical Security Requirements**
3. Offices shall be sited to avoid access from unauthorized individuals and shall be secured.
4. All Service provider's information processing facilities must be physically sound in design and consider landscaping, lighting, fencing, and closed-circuit television on the access routes to the building; that the roof, walls, and flooring are of solid construction; and that exterior access points, windows, and doors are equipped with appropriate security controls (e.g., locks, alarms, bars).

1. **Physical Security Perimeter**
2. Security perimeters of the building or site containing information processing facilities shall depend upon the classification of the information resources within.
3. **Physical Entry Controls**
4. The premises will be controlled with Biometric Access Control where applicable
5. Employees will have access to designated areas only
6. Upon dismissal of employees, access to the premises shall be immediately revoked
7. The Biometric Access Control system shall keep a log of all activities, entry, and egress
8. Privileges to be monitored annually
9. Dormant account control – specifically, personnel that have not accessed the system for 60 consecutive days shall automatically be suspended
10. **Alarm**
11. The premises shall maintain a Primary Alarm, to be switched on after-hours
12. The alarm is linked to a security control room.
13. Testing must be recorded by the person receiving the signal in the control room
14. If an alarm failed to trigger, a report must be drafted, and a corrective action plan followed.
15. Alarms to be tested monthly
16. When the alarm registers, the appropriate Regional Manager, Branch Manager, or Facilities Manager must be notified via SMS.
17. **Maintenance**
18. No aircon units to be installed above a server
19. Aircons must be serviced bi-annual
20. Generator/ UPS shall be serviced
21. Facilities Manager shall ensure enough diesel/fuel is kept on site
22. The server room shall be cleaned
23. Computer equipment being repaired or maintained must be protected corresponding with the sensitivity of the information it contains and the value of the equipment.
24. Maintenance of systems, hardware, or media containing information - Information Owners shall consider the sensitivity of the information stored on hardware or media when determining whether repairs will be conducted.
25. **Secure Areas**
26. Only authorized employees are allowed access and where relevant signage shall be placed to advise of secure areas and authorized employees entry only.
27. Existing secure areas that require special rules are the server room and is only accessible to personnel specified on the Server Room Access Information document where applicable.
28. Access to secure areas is approved according to the Access Control Policy.
29. Access to secure areas is protected with biometrics.

**Access of visitors**

1. Persons who are not employed must obtain access according to the Access Control Policy.
2. Visitors may enter the secure areas and stay in those areas only in the presence of a host who shall accompany the visitor throughout their whole stay in the secure area.

**Prohibited activities**

Within secure areas, it is not allowed to:

1. perform any kind of photographic, audio, or video recording;
2. plug any electrical device into a power supply unless specifically authorized to do so;
3. touch or in any other way tamper with any equipment installed in secure areas unless specifically authorized to do so;
4. connect any device to a network unless specifically authorized to do so;
5. archive a larger amount of paper materials;
6. store flammable materials or equipment;
7. use any kind of heating devices;
8. smoke, eat or drink.
9. **Protecting Against External and Environmental Threats**
10. Service providers and their site planners and architects must incorporate physical security controls, which require protection against damage from fire, flood, and other forms of natural disasters, malicious acts, and accidents. Consideration must be given to any security threats presented by neighboring premises or streets.

1. Rules for working in secure areas shall be as stated above to prevent unauthorized physical access to service provider's information processing facilities and unsupervised work in secure areas.
2. **Delivery and Loading Areas**
3. Access from reception is controlled by access cards and a full-time receptionist to prevent unauthorized access.
4. **Cabling Security (Including Data Centers)**
5. Power and telecommunications cabling carrying data or supporting information services is protected from interception, interference, or damage.
6. **Removal of Equipment**
7. Equipment designated for removal must be recorded.
8. **Security of Equipment and Assets Off-Premises**
9. Employees are responsible for the physical protection of mobile computing equipment and must take special care when equipment is placed in, or used in, cars or other forms of transportation, public spaces, hotel rooms, meeting places, conference centers, and other unprotected areas outside Vital College premises.
10. Employees must ensure that computing equipment being used offsite to access Vital College information is protected proportional to the sensitivity and the value of the information it contains.
11. Employees must guard against unauthorized persons reading their computer or mobile computing device screen when in a public place.

1. **References**

|  |
| --- |
| **Document Name** |
| ISO/IEC 27001 standard, clauses A.11.1.5 |
| Server Room Access Information |
| Access Control Policy |

1. **Outputs**

The following records need to be kept and stored securely.

|  |  |  |  |
| --- | --- | --- | --- |
| **Record** | **Responsible Person** | **Retention** | **Disposition** |
| Physical Security Register |  |  |  |
| Equipment removal register |  |  |  |
|  |  |  |  |

All records must be stored in the pre-allocation location. All physical copies need to be stored in a lockable cabinet or drawer.

1. **Enforcement**

An employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment. A violation of this policy by a temporary worker, contractor, or vendor may result in the termination of their contract or assignment with Vital College.

Any exception to the policy must comply with the **Exceptions Policy**.

1. **Definitions**

|  |  |
| --- | --- |
| **TERMS** | **DESCRIPTION** |
|  |  |

A black and white drawing of a handwritten note

Description automatically generated with low confidence

**DIRECTOR name** Duncan MacNicol **DIRECTOR signature**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**Signed at** Durban **on this** 20th day of February 2021



|  |  |  |
| --- | --- | --- |
|  | **Vital College (Pty) Ltd** | |
| Authorised by: | Duncan MacNicol |
| Date Authorised: | 20 February 2021 |
| Document Number: | VC-022 |

**POPI and Privacy Policy**

1. **Introduction**
2. **Overview**

* Where**we** refer to “process”, it means how **we** collect, use, store, make available, destroy, update, disclose, or otherwise deal withpersonal information. As a general rule **we** will only process this personal information if it is required to deliver or offer a service, provide a product, carry out a transaction or obligation in a contract.
* **We** may combine thispersonal information and use the combined personal information for any of the purposes stated in this Privacy Policy.
* If **you**use **our** other services, goods, products, and service channels **you** agree that **we**may process this personal information as explained under this Privacy Policy. Sometimes **you** may provide **us** with consent to process this personal information.
* Vital Collegeis a global organisation and as such this Privacy Policy will apply to the processing of personal information by any member of Vital Collegeglobally. If Vital Collegeprocesses personal information for another party under a contract or a mandate, the other party’s privacy policy will apply to the processing of such information.
* Vital College can change this Privacy Policy from time to time if the law or **our** business practices requires such change.
* This policy establishes a general standard for the appropriate protection of personal information (POPI) within the Vital Collegeenvironment furthermore, it provides principles regarding the rights of individuals to privacy and to reasonable safeguards of their personal information.

1. **Scope**

All employees, contractors, consultants, temporary and other workers at Vital College, including all personnel affiliated with third parties must adhere to this policy. This policy applies to information assets owned or leased by Vital College, or to devices that connect to a Vital College network or reside at an Vital College site.

1. **Policy Statement**
2. **What is personal information?**

Personal information refers to any information that identifies **you** or specifically relates to **you**, or **your** employees stored or processed on **The Product/s**. Personal information includes, but is not limited to, the following information about **you** and / or **your**employees:

* Marital status
* National origin
* Age
* Language
* Birthplace
* Education
* Relevant financial history
* Identifying number (like an employee number, identity number or passport number)
* E-mail address; physical address (like residential address, work address or your physical location); telephone number
* Biometric information (like fingerprints, signature, or voice)
* Race; gender; sex; pregnancy status; ethnic origin; social origin; colour; sexual orientation
* Physical health; mental health; well-being; disability; religion; belief; conscience; culture
* Medical history; criminal history; employment history
* Personal views, preferences, and opinions
* Another’s views or opinions about you
* Full names and initials

Personal information includes special personal information, as explained below.

1. **When will we process your personal information?**

**We** will only process this personal information for lawful purposes relating to **our**business if the following applies:

* If **you**have consented thereto
* If a person legally authorised by **you**, the law, or a court, has consented thereto
* If it is necessary to conclude or perform under a contract, **we** have with **you**
* If the law requires or permits, it
* If it is required to protect or pursue **your**, **our** or a third party’s legitimate interest

1. **What is special personal information?**

Special personal information is personal information about the following:

* Race (like where a company submits reports to the Department of Labour where the statistical information must be recorded)
* Ethnic origin
* Trade union membership
* Health (like where you apply for an insurance policy)
* Biometric information (like to verify your identity); and / or your criminal behaviour and alleged commission of an offense

1. **When will we process your special personal information?**

We may process **your** special personal information in the following circumstances:

* If **you** have consented to the processing
* If the information is being used for any Human Resource or payroll related requirement
* If the processing is needed to create, use or protect a right or obligation in law
* If the processing is for statistical or research purposes and all legal conditions are met
* If the special personal information was made public by **you**
* If the processing is required by law

1. **When and from where we obtain personal information about you**

* **We** collect personal information from you directly.
* We may collect personal information from a public record or if you have deliberately made the information public.
* **We** collect personal information from 3rd parties that are directly integrated with **our** software platform
* **We** collect information about **you** based on **your** use of **our** products, services, or service channels.
* **We** collect information about **you** based on how **you** engage or interact with **us** such as via emails, letters, telephone calls and surveys
* We collect personal information from completed forms i.e., contact and billing information

If the law requires **us** to do so, we will ask for **your** consent before collecting personal information

The third parties from whom **we** may collect **your**personal information include, but are not limited to, the following:

* **Our** partners, **your** employer, employees directly, any of **our** other Bureau or channel partners and any connected companies, subsidiary companies, its associates, cessionaries, delegates, assigns, affiliates or successors in title and / or appointed third parties (like its authorised agents, partners, contractors and suppliers) for any of the purposes identified in this Privacy Policy.
* **your** spouse, dependents, partners, employer, and other similar sources.
* people **you** have authorised to share **your** personal information, like a person that makes a travel booking on **your**behalf or a medical practitioner for insurance purposes.
* attorneys, tracing agents, debt collectors and other persons that assist with the enforcement of agreements.
* payment processing services providers, merchants, banks, and other persons that assist with the processing of **your** payment instructions, like EFT transaction partners.
* insurers, brokers, other financial institutions, or other organisations that assist with insurance and assurance underwriting, the providing of insurance and assurance policies and products, the assessment of insurance and assurance claims and other related purposes.
* law enforcement and fraud prevention agencies and other persons tasked with the prevention and prosecution of crime.
* regulatory authorities, industry ombudsman, governmental departments, local and international tax authorities.
* trustees, Executors or Curators appointed by a court of law.
* **our** service providers, agents and sub-contractors like couriers and other persons **we** use to offer and provide products and services to **you**.
* courts of law or tribunals.

1. **Reasons we need to process your personal information**

**We** will process **your** personal information for the following reasons:

* to provide **you** with products, goods and services.
* to market **our** products, goods and services to **you**.
* to respond to **your** enquiries and complaints.
* to comply with legislative, regulatory, risk and compliance requirements (including directives, sanctions and rules), voluntary and involuntary codes of conduct and industry agreements or to fulfil reporting requirements and information requests.
* to conduct market and behavioural research, including scoring and analysis to determine if **you** qualify for products and services or to determine **your** credit or insurance risk.
* to develop, test and improve products and services for **you**.
* for historical, statistical and research purposes, like market segmentation.
* to process payment instruments;
* to create manufacture and print payment advice.
* to enable **us** to deliver goods, documents, or notices to **you**.
* for security, identity verification and to check the accuracy of **your** personal information.
* to communicate with **you** and carry out **your** instructions and requests.
* for customer satisfaction surveys, promotional offerings.
* to enable you to take part in and make use of value-added products and services.
* to assess our lending and insurance risks; and / or
* for any other related purposes.

1. **How we use your personal information for marketing purposes**

* **We**will use your personal information to market our services, related products, and services to **you**
* **We**may also market non-banking or non-financial products, goods, or services to you
* **We** will do this in person, by post, telephone, or electronic channels such as SMS, email, and fax
* If **you** are not **our**customer, or in any other instances where the law requires, **we** will only market to **you** by electronic communications with **your** consent
* In all cases **you** can request **us** to stop sending marketing communications to **you** at any time

1. **When how and with whom we share your personal information**

In general, we will only share **your**personal information if any one or more of the following apply:

* If **you** have consented to this
* If it is necessary to conclude or perform under a contract, **we** have with **you**
* If the law requires it; and / or
* If it’s necessary to protect or pursue **your**, our or a third party’s legitimate interest

Where required, each member of Vital Collegemay share **your** personal information with the following persons. These persons have an obligation to keep **your** personal information secure and confidential.

* Other members of Vital College, its associates, cessionary, delegates, assigns, affiliates or successors in title and / or appointed third parties (like its authorised agents, partners, contractors and suppliers) for any of the purposes identified in this Privacy Policy
* **Our** employees as required by their employment conditions
* Attorneys, tracing agents, debt collectors and other persons that assist with the enforcement of agreements
* Payment processing services providers, merchants, banks, and other persons that assist with the processing of **your**payment instructions, like 3rd party EFT service providers
* Law enforcement and fraud prevention agencies and other persons tasked with the prevention and prosecution of crime
* Regulatory authorities, industry ombudsmen, governmental departments, local and international tax authorities, and other persons the law requires **us** to share **your** personal information with
* **Our** service providers, agents and sub-contractors like couriers and other persons **we** use to offer and provide products and services to **you**
* Persons to whom **we** have ceded our rights or delegated our obligations to under agreements, like where a business is sold
* Courts of law or tribunals that require the personal information to adjudicate referrals, actions, or applications.
* Trustees, Executors or Curators appointed by a court of law
* Participating partners in **our**customer loyalty reward programmes, where **you** purchase goods, products and service or spend loyalty rewards; and / or our joint venture and other partners with whom **we** have concluded business agreements, for **your**benefit

1. **Under what circumstances will we transfer your information to other countries?**

**We** will only transfer **your** personal information to third parties in another country in any one or more of the following circumstances:

* Where **your** personal information will be adequately protected under the other country’s laws or an agreement with the third-party recipient
* Where the transfer is necessary to enter into or perform under a contract with **you**, or a contract with a third party that is in **your** interest
* Where **you** have consented to the transfer; and / or
* Where it is not reasonably practical to obtain **your** consent, the transfer is in **your** interest

This transfer will happen within the requirements and safeguards of the law. Where possible, the party processing **your** personal information in the other country will agree to apply the same level of protection as available by law in **your** country or if the other country’s laws provide better protection the other country’s laws would be agreed to and applied.

An example of **us** transferring **your** personal information to another country is where foreign payments take place if **you**purchase goods or services in a foreign country, or request that **we** facilitate salary payments to **your** employees in the countries.

1. **Your duties and rights about the personal information we have about you**

**You**must provide proof of identity when enforcing the rights below.

**You**must inform **us** when **your** personal information changes.

Please refer to our Promotion of Access to Information Act 2 of 2000 Manual ([PAIA Manual](http://www.justice.gov.za/inforeg/docs/InfoRegSA-POPIA-act2013-004.pdf)) for further information on how **you** can give effect to the rights listed below.

**You** have the right to request access to the personal information **we** have about **you** by contacting **us**. This includes requesting:

· Confirmation that we hold **your** personal information   
· A copy or description of the record containing **your** personal information; and   
· The identity or categories of third parties who have had access to **your** personal information

**We**will attend to requests for access to personal information within a reasonable time. **You** may be required to pay a reasonable fee to receive copies or descriptions of records, or information about third parties. **We**will inform **you** of the fee before attending to **your** request.

Please note that the law may limit **your** right to access information.

**You** have the right to request **us** to correct or delete the personal information **we** have about **you**if it is inaccurate, irrelevant, excessive, out of date, incomplete, misleading, obtained unlawfully or **we** are no longer authorised to keep it. **You** must inform **us**of **your** request in writing. Please refer to our PAIA Manual for further information in this regard, like the process **you** should follow to give effect to this right. It may take up to 15 business days for the change to reflect on our systems. **We** may request documents from **you** to verify the change in personal information.

A specific agreement that **you**have entered into with **us** may determine how **you** must change **your** personal information provided at the time when **you** entered into the specific agreement. Please adhere to these requirements. If the law requires **us** to keep the personal information, it will not be deleted upon **your**request. The deletion of certain personal information may lead to the termination of **your** relationship with **us**.

**You** may object on reasonable grounds to the processing of **your** personal information.

**We** will not be able to give effect to **your** objection if the processing of **your**personal information was and is permitted by law; **you** have provided consent to the processing and **our** processing done according to **your** consent or the processing is necessary to conclude or perform under a contract with **you**.

**You** must inform **us** of any objection in writing. Please refer to **our** PAIA Manual for further information in this regard, like the process **you** should follow to give effect to this right.

Where **you**have provided **your** consent for the processing of **your**personal information, **you** may withdraw **your** consent. If **you** withdraw **your** consent, **we** will explain the consequences to **you**. **We** may proceed to process **your** personal information even if **you** have withdrawn **your** consent if the law permits or requires it. It may take up to 15 business days for the change to reflect on **our** systems, during this time **we** may still process **your** personal information.

**You** have a right to file a complaint with **us**or any Regulator with jurisdiction about an alleged contravention of the protection of **your** personal information by us. **We**will address **your** complaint as far as possible.

1. **How we secure your personal information**

**We** will take appropriate and reasonable technical and organisational steps to protect **your** personal information according to industry best practices. **Our** security measures (including physical, technological and procedural safeguards) will be appropriate and reasonable. This includes the following:

* Keeping **our**systems secure (like monitoring access and usage)
* Storing **our** records securely
* Controlling the access to **our** buildings, systems and/or records; and
* Safely destroying or deleting records
* Ensure compliance with international security standards

1. **How long do we keep your personal information?**

**We** will keep **your** personal information for as long as:

* The law requires **us** to keep it
* A contract between **you** and **us** requires **us** to keep it
* **You** have consented to **us** keeping it
* **We**are required to keep it to achieve the purposes listed in this Privacy Policy
* **We** require it for statistical or research purposes
* A code of conduct requires **us**to keep it; and / or
* **We** require it for our lawful business purposes

Note: **We**may keep **your p**ersonal information even if **you** no longer have a relationship with **us**, for the historical data that may be required by **your** employer or employee.

1. **Children's Privacy**

Our Service does not address anyone under the age of 13. We do not knowingly collect personally identifiable information from anyone under the age of 13. If You are a parent or guardian and You are aware that Your child has provided Vital College with Personal Data, please contact Us. If We become aware that We have collected Personal Data from anyone under the age of 13 without verification of parental consent, we take steps to remove that information from Our servers.

If We need to rely on consent as a legal basis for processing Your information and Your country requires consent from a parent, we may require Your parent's consent before We collect and use that information.

1. **Our cookie policy**

A cookie is a small piece of data sent from **our** websites or applications to **your** computer or device hard drive or Internet browser where it is saved. The cookie contains information to personalise **your** experience on **our** websites or applications and may improve **your** experience on the websites or applications. The cookie will also identify **your** device, like the computer or smart phone.

By using **our** websites or applications **you** agree that cookies may be forwarded from the relevant website or application to **your**computer or device. The cookie will enable **us** to know that **you** have visited the website or application before and will identify **you**. **We** may also use the cookie to prevent fraud and for analytics.

1. **References**

|  |
| --- |
| **Document Name** |
| Information Classification Policy |
| PAIA Manual |
|  |
|  |
|  |
|  |

1. **Outputs**

The following records need to be kept and stored securely.

|  |  |  |  |
| --- | --- | --- | --- |
| **Record** | **Responsible Person** | **Retention** | **Disposition** |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

All records must be stored in the pre-allocation location. All physical copies need to be stored in a lockable cabinet or drawer.

1. **Enforcement**

An employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment. A violation of this policy by a temporary worker, contractor, or vendor may result in the termination of their contract or assignment with Vital College.

Any exception to the policy must comply with the **Exceptions Policy**.

1. **Definitions**

|  |  |
| --- | --- |
| **TERMS** | **DESCRIPTION** |
|  |  |

A black and white drawing of a handwritten note

Description automatically generated with low confidence

**DIRECTOR name** Duncan MacNicol **DIRECTOR signature**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**Signed at** Durban **on this** 20th day of February 2021



|  |  |  |
| --- | --- | --- |
|  | **Vital College (Pty) Ltd** | |
| Authorised by: | Duncan MacNicol |
| Date Authorised: | 20 February 2021 |
| Document Number: | VC-023 |

**Removable Media Policy**

1. **Introduction**
   1. **Overview**

Removable media is a well-known source of malware infections and has been directly tied to the loss of sensitive information in many organizations. The purpose of this policy is to minimize the risk of loss or exposure of sensitive information maintained by Vital College and associates and to reduce the risk of acquiring malware infections on computers operated by Vital College and associates.

* 1. **Scope**

This policy covers all computers and servers operating within Vital College environment.

1. **Policy Statement**
   1. **Policy**

Vital College staff may only use Vital College removable media in their work computers. Removable media may not be connected to or used in computers that are not owned or leased by the Vital College without the explicit permission of the Labour Net IT Department. Removable media pose a threat and need to be scanned for malware infections prior to connecting the media to a corporate computer and/or server.

Sensitive information should be stored on removable media only when required in the performance of your assigned duties or when providing client information directly to the client. When sensitive information is stored on removable media, it must be encrypted as per the **Acceptable Encryption Policy.**

Information stored on removable media must be destroyed after the intended use and musk not be kept for backup purposes. The disposal of removable media must comply with the Technology Disposal Policy.

For security, compliance, and maintenance purposes, authorized personnel may monitor and audit equipment, systems, and network traffic as per the **Acceptable Use Policy.**

Exceptions to this policy may be requested on a case-by-case basis as per the **Exception Policy**.

**References**

|  |
| --- |
| **Document Name** |
| Acceptable Encryption Policy |
| Acceptable Use Policy |
| Exception Policy |
| Technology Disposal Policy |

**Outputs**

The following records need to be kept and stored securely.

|  |  |  |  |
| --- | --- | --- | --- |
| Record | Responsible Person | Retention | Disposition |
| Approvals for removeable media |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

All records must be stored in the pre-allocation location. All physical copies need to be stored in a lockable cabinet or drawer.

**Enforcement**

An employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment. A violation of this policy by a temporary worker, contractor or vendor may result in the termination of their contract or assignment with Vital College

Any exception to the policy must comply with the **Exceptions Policy.**

**Definitions**

|  |  |
| --- | --- |
| **Terms** | **Description** |
| **Removable media** | Removable media is any type of storage device that can be removed from a computer while the system is running. Examples of removable media include CDs, DVDs, and Blu-ray disks, as well as diskettes and USB drives. Removable media makes it easy for a user to move data from one computer to another. Mobile phones are also considered Removable Media |
| **Encryption** | In cryptography, encryption is the process of encoding a message or information in such a way that only authorized parties can access it and those who are not authorized would not be able to view the information. Encryption does not itself prevent interference but denies the intelligible content to a would-be interceptor. |
| **Malware** | Malware, or malicious software, is any program or file that is harmful to a computer and or IT network. Types of malwares can include computer viruses, worms, trojan horses and spyware. |

A black and white drawing of a handwritten note

Description automatically generated with low confidence

**DIRECTOR name** Duncan MacNicol **DIRECTOR signature**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**Signed at** Durban **on this** 20th day of February 2021

|  |  |  |
| --- | --- | --- |
| C:\Users\JReddy\AppData\Local\Microsoft\Windows\INetCache\Content.Word\Vital small simple.jpg | **Vital College (Pty) Ltd** | |
| Authorised by: | Duncan MacNicol |
| Date Authorised: | 20 February 2021 |
| Document Number: | VC-024 |

**Request for Policy/Procedure Exception**

|  |  |  |  |
| --- | --- | --- | --- |
| **Contact Information** | | | |
| **Name & Surname** |  | | |
| **Job Title** |  | | |
| **Date** |  | | |
| **Signature** |  | | |
| **Exception Information** | | | |
| **Exception** |  | | |
| **Policy or procedure to which exception applies:** |  | | |
| **Detailed explanation regarding the reason for exception:** |  | | |
|  | | |
|  | | |
|  | | |
| **Describe potential risks or implications introduced by this exception:** |  | | |
|  | | |
|  | | |
| **Duration of Exemption** |  | | |
|  | | |
| **Authorizations** | | | |
| **Signature of Process Owner** | **Signature Executive Authorization** | | |
|  |  | | |
| **Date** | **Date** | | |
|  |  | | |
|  |  | | |
|  | | **Vital College (Pty) Ltd** | | |
| Authorised by: | Duncan MacNicol | |
| Date Authorised: | 20 February 2021 | |
| Document Number: | VC-025 | |



**Risk Assessment and Risk Treatment Methodology Policy**

1. **Introduction**
2. **Overview**

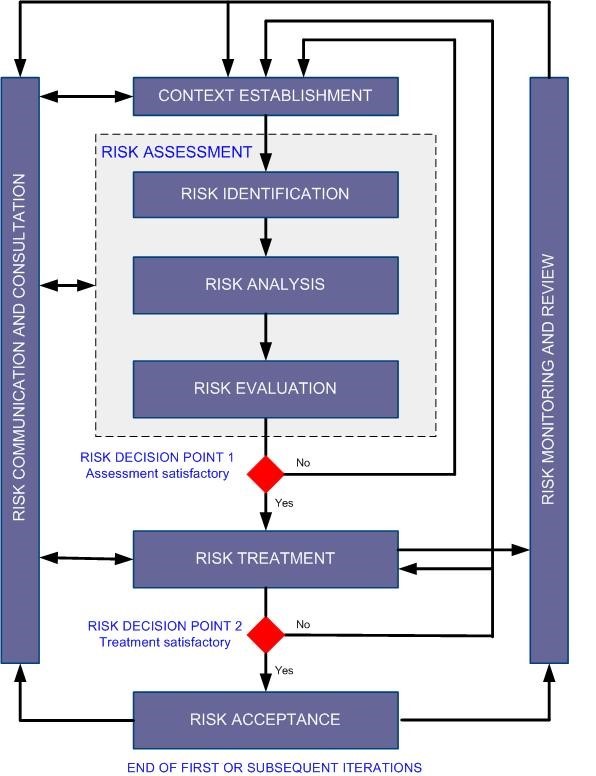
The purpose of this document is to define the methodology for assessment and treatment of information risks in Vital College, and to define the acceptable level of risk according to the ISO/IEC 27001 standard.

Risk assessment and risk treatment are applied to the entire scope of the Information Security Management System (ISMS), i.e. to all assets which are used within the organization or which could have an impact on information security within the ISMS.

1. **Responsibilities and Authorities**

Executive Management.

1. **Procedure**
2. **The Risk Management Process**

****

1. **Process Steps**
2. The context is established first.
3. Then a risk assessment is conducted.
4. If this provides sufficient information to effectively determine the actions required to modify the risks to an acceptable level, then the task is complete, and the risk treatment follows.
5. If the information is insufficient, another iteration of the risk assessment with revised context (e.g. risk evaluation criteria, risk acceptance criteria or impact criteria) will be conducted, possibly on limited parts of the total scope.
6. The effectiveness of the risk treatment depends on the results of the risk assessment.
7. Note that risk treatment involves a cyclical process of:
8. assessing a risk treatment.
9. deciding whether residual risk levels are acceptable.
10. generating a new risk treatment if risk levels are not acceptable; and
11. assessing the effectiveness of that treatment
12. The risk acceptance activity must ensure residual risks are explicitly accepted by the responsible managers, especially in a situation where the implementation of controls is omitted or postponed, e.g. due to cost.
13. During the whole information security risk management process, it is important that risks and their treatment are communicated to the appropriate managers and operational staff. Even before the treatment of the risks, information about identified risks can be very valuable to manage incidents and may help to reduce potential damage. Awareness by managers and staff of the risks, the nature of the controls in place to mitigate the risks and the areas of concern to the organization assist in dealing with incidents and unexpected events in the most effective manner.
14. The detailed results of every activity of the information security risk management process and from the two risk decision points should be documented.
15. ISO/IEC 27001 specifies that the controls implemented within the scope, boundaries and context of the ISMS need to be risk based.

1. **Writing a good Risk Statement**
2. Components or characteristics that may make up a risk including:
3. Event – The conditions that must be present for the risk to occur.
4. Likelihood – The probability that the conditions for the event will occur.
5. Outcome – What will happen when the conditions are present.
6. Impact –  What is the harm that will result from the outcome?
7. Risk Factors – The conditions that increase the likelihood of the event and/or the harm from the impact.
8. Control – A limiting factor that reduces the likelihood of the event and/or the harm from the impact.
9. At a minimum, a risk needs an Event that leads to an Outcome that results in an Impact. So, a minimal risk statement could be formed as: There is a risk that <event> occurs leading to <outcome> that causes <impact>.
10. An example of a minimal risk structured as above is: “There is a risk that a member of staff accidentally emails financially sensitive data to an external recipient leading to a data breach which results in regulatory enforcement.”
11. This risk statement could be supported with risk factors and control characteristics such as: “The financially sensitive data is marked sensitive information before the annual report is published, but the data leakage control is configured to look for financial reports and to prevent their external transmission, and the Outlook autocomplete function is disabled for the period of the production of the annual report.

1. **Risk Assessment**
2. Risk assessment is implemented through ISMS Risk Register. The risk assessment process is coordinated by the IT department, identification of risks and assessment of consequences and likelihood is performed by risk owners.
3. Fields in the ISMS Risk Register worksheet should be filled in as per following definitions and guidelines

|  |  |
| --- | --- |
| **Field Name** | **Definition / Instructions** |
| Risk ID | Running serial number. Number should be assigned sequentially every time a new risk is identified. |
| Date Risk Raised | Date risk raised |
| Raised by | Person raising the risk |
| Risk Owner | The owner of the risk |
| Risk Statement | Statement of the potential risk |
| CIA | risks associated identified with the loss of confidentiality, integrity, and availability of information within the scope of the ISMS |
| Current Risk Comments | Comments / remarks to qualify / explain existing controls in place. Also comments to explain / qualify any recommendations for risk acceptance |
| Controls areas for existing controls | List of control numbers from the standard ISO 27001 Annex A that correspond to the existing controls in place |
| Current Risk Probability/ Likelihood | Probability or likelihood of existing occurring considering existing controls in place. |
| Current Risk Impact/Consequence | Consequence or impact of existing risk without new treatment measures if the risk eventuates. Refer to Risk Criteria |
| Risk Exposure (Risk Factor) | * Risk Likelihood x Risk Consequence. * Risk acceptance criteria: * Low and Medium values are acceptable risks, while * High, Very High, and Critical values unacceptable risks. * Unacceptable risks must be treated. |
| Risk Treatment Decision | * **Terminate/Avoid:** If a risk is deemed too high, then you simply avoid the activity that creates the risk.      * **Transfer:**E.g. insurance, outsource the process in which the risk is present to another provider, thereby transferring the risk to the outsource provider with contracts and service level agreements.      * **Treat/Reduce:** Risk reduction is one of the most crucial steps for processes or activities that cannot be avoided, and where risk cannot be transferred to another party. E.g training your staff on how to identify a phishing email, or on best practices involving login credentials and password hygiene.      * **Tolerate/Accept:** E.g processes and activities where there is no option but to accept the risk. Of course, these instances should only involve low risk, or repercussions that are easily managed. Some risks might be completely acceptable and require you to take no action at all |
| Risk Treatment Plan | Comments / remarks to qualify / explain new treatment measures being proposed / applied |
| Describe possible controls | * List of the relevant control area from the standard ISO27001 Annex A that correspond to the new treatment measures proposed / applied. * When several security controls are selected for a risk, then additional rows are inserted into the table immediately below the row specifying the risk. * The treatment of risks related to outsourced processes must be addressed through the contracts with responsible third parties, as specified in ISMS-05 Supplier Information Security Policy. |
| Possible Control References | * List of control numbers from the standard ISO 27001 Annex A that correspond to the existing controls in place |
| Treated/Residual Risk Consequence | * Consequence or impact of treated risk assuming the recommended treatment measures have been applied. Possible values 1 to 5. * Refer to "Risk Category" table for definition. |
| Treated/Residual Risk Likelihood | * Assess the new value of consequence and likelihood in the Risk Treatment Table, in order to evaluate the effectiveness of planned controls. * Probability or likelihood of treated risk occurring assuming the recommended treatment measures have been applied. Possible values **1** to **5**. * Refer to "Risk Category" table for definition. |
| Treated/Residual Risk Rating | * Rating or exposure of treated residual risk considering the treatment measure(s) has been applied if the risk eventuates. * Refer to "Risk Category" worksheet for possible values and definitions. |
| Date of Risk Owner's Acceptance/Treatment Approval | Date when the Risk Owner accepted the risk or approved the treatment plan |
| Risk Treatment Owner | * Person accountable for implementing the treatment plan * At least annual review of existing risks and update the Risk Assessment Table and Risk Treatment Table in line with newly identified risks. * Review more frequently in the case of significant organizational changes, significant change in technology, change of business objectives, changes in the business environment, etc. |
| Date Risk Treatment due | * Planned implementation date of risk treatment plan / new control |
| Date Risk Treatment implemented | * Actual implementation date of risk treatment plan / new control |
| Reviewed | * The organization shall perform information security risk assessments at planned intervals or when significant changes are proposed or occur. |

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **The table below forms the basis for risk assessment for the ISMS in conjunction with the Risk Management Policy** | | | | | | | | |
|  |  | |  | |  | |  |  |
| **Current / Treated Risk Matrix** | | | | | | | | |
|  |  | |  | |  | |  |  |
| **Level of Probability** | **Level of Consequence/Impact** | | | | | | | |
| **1**  (Insignificant) | **2**  (Minor) | | **3**  (Moderate) | | **4**  (Major) | | **5**  (Catastrophic) |
| **5** (Almost Certain) | Medium | High | | Very High | | Critical | | Critical |
| **4**(Probable) | Medium | High | | Very High | | Critical | | Critical |
| **3**(Possible) | Low | Medium | | High | | Very High | | Very High |
| **2** (Improbable) | Low | Low | | Medium | | High | | High |
| **1**(Rare) | Low | Low | | Low | | Medium | | Medium |
|  |  |  | |  | |  | |  |

|  |  |  |
| --- | --- | --- |
| **Consequence/Impact** | | **Description** |
| **1** | Insignificant:  Minimal operational impact | Loss of confidentiality, availability or integrity does not affect the organization's cash flow, legal or contractual obligations, or its reputation. |
| **2** | Minor:  Minimal operational impact | < R50 000, legal or contractual obligations, or its reputation. |
| **3** | Moderate:  Remedial action required | Incurs costs <R100 000 and has a low or moderate impact on legal or contractual obligations, or the organization's reputation. |
| **4** | Major:  Loss of operational capability | Has considerable and/or immediate impact. Incurs costs <R500 000, operations, has reputational, legal or contractual impact |
| **5** | Catastrophic:  Unacceptable, operational failure | Incurs costs >R500 000, loss of client, operational failure |

|  |  |  |  |
| --- | --- | --- | --- |
|  | **Probability/Likelihood** | | **Description** |
|  | **5** | Almost certain  > 60% - < 80%  (e.g. Every day) | No strategy or current strategy will resolve this issue. Existing security controls are low or ineffective. Such incidents have a high likelihood of occurring in the future. Alternatives will be required, mitigation actions urgently to be done. |
|  | **4** | Likely/probable  > 40% - 60%  (e.g. Once a week) | Current strategy will probably not resolve this issue.  Alternatives will be required, mitigation actions needed. |
|  | **3** | Moderate/Possible  > 20 to 40%  (e.g. Once a month) | Current strategy may not resolve this issue.  Alternatives may be required; mitigation actions are to be considered. Existing security controls are moderate and have mostly provided an adequate level of protection. New incidents are possible, but not highly likely. |
|  | **2** | Unlikely/Improbable  > 5 to 20% | Current strategy should resolve this issue. |
|  | **1** | Rare  5% or less  (e.g. once a year) | Current actions are in order. Issue can be resolved quickly and easily. Existing security controls are strong and have so far provided an adequate level of protection. No new incidents are expected in the future. |
| **Risk Categories** | | | | |
| Strategic Risks: | | Strategic impact should they materialize.  The subcategories are: Economic, Organization Planning, Reputation, Business Relations, Market Structure and Market Dynamics. | | |
| Financial Risks: | | Financial impact should they materialize.  The subcategories are:  Credit, Reporting, Market and Liquidity. | | |
| Business and Operational Risks: | | Financial impact should they materialize.  The subcategories are:  Information Management, Legal Risk, Business Continuity, HR, Process, System and Client Satisfaction. | | |
| Compliance Risk: | | Financial impact should they materialize.  The subcategories are:  Legal Compliance, Governance Risk, Certification Risk and Financial Compliance | | |

1. **Statement of Applicability**
2. The Enterprise Solutions Architect must document the Statement of Applicability to identify which security controls from Annex A of the ISO/IEC 27001 standard are applicable and which are not as identified in the risk assessment, the justification for such decisions, and whether they are implemented or not.
3. On behalf of the risk owners, executive management will accept all residual risks through the Statement of Applicability.

1. **Reporting**
2. The Compliance will document the results of risk assessment and risk treatment, and all the subsequent reviews, in the Risk Assessment and Treatment Report.
3. The Compliance will monitor the progress of implementation of the Risk treatment plan and report the results to the IT Executive each month.

1. **References**

|  |
| --- |
| **Document Name** |
| ISO/IEC 27001 standard, clauses 6.1.2, 6.1.3, 8.2, and 8.3 |
| Information Security Policy |
| List of Legal, Regulatory and Contractual and Other Requirements |
| Statement of Applicability |
|  |
|  |

1. **Outputs**

The following records need to be kept and stored securely.

|  |  |  |  |
| --- | --- | --- | --- |
| **Record** | **Responsible Person** | **Retention** | **Disposition** |
| ISMS Risk Register (electronic form – Excel document) | Compliance | Indefinite | n/a |
| SOA | Compliance | 2 Years | n/a |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

All records must be stored in the pre-allocation location. All physical copies need to be stored in a lockable cabinet or drawer.

1. **Definitions**

|  |  |
| --- | --- |
| **TERMS** | **DESCRIPTION** |
|  |  |

A black and white drawing of a handwritten note

Description automatically generated with low confidence

**DIRECTOR name** Duncan MacNicol **DIRECTOR signature**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**Signed at** Durban **on this** 20th day of February 2021



|  |  |  |
| --- | --- | --- |
|  | **Vital College (Pty) Ltd** | |
| Authorised by: | Duncan MacNicol |
| Date Authorised: | 20 February 2021 |
| Document Number: | VC-026 |

**Security Incident Response Plan**

1. **Introduction**
2. **Overview**

This procedure aims to ensure that all such Security Incidents are detected, analysed, contained, and eradicated, that measures are taken to prevent any further Security Incidents, and, where necessary or appropriate, that notice is provided to law enforcement authorities, Personnel, and/or affected parties. This document is a step-by-step guide of the measures Personnel are required to take to manage the lifecycle of Security Incidents within Vital College, from initial Security Incident recognition to restoring normal operations.

1. **Scope**

The purpose of this document is to define the Incident Response procedures followed by Vital College in the event of a Security Incident.

This document covers the Incident Response process for all identified Security Incidents. The following activities will be covered:

• Detection

• Analysis

• Containment

• Eradication

• Recovery

• Post-Incident Activities

The Incident Response process is considered complete once Information confidentiality, integrity, and/or availability are restored to normal, and verification has occurred.

1. **Procedure**
2. **Roles and Responsibilities**

Individuals needed and responsible for responding to a Security Incident make up the Security Incident Response Team. Core members will include the following:

• Security Team Lead (SIRT Primary Lead)

• Legal & Compliance (SIRT Secondary Lead)

• Security team staff

• Information owner

Other groups and/or individuals that may needed to be include:

• Senior management

• Human Resources

• End User Support

• Dev Ops Staff

• Building and/or facilities management staff

• Other Personnel involved in the Security Incident or needed for resolution

• Contractors (as necessary)

• Communications Resources

1. **Process**

**Diagram

Description automatically generated**

1. **Detection Phase**

In the detection phase the Security Incident Response Team (SIRT), or an internal or external entity, identifies a Security Event that may be the result of a potential exploitation of a Security Vulnerability or a Security Weakness, or that may be the result of an innocent error.

1. Immediately upon observation or notice of any suspected Security Event, Personnel shall use reasonable efforts to promptly report such knowledge and/or suspicion to the Information Security Department.
2. A Security Event may be discovered in many ways, including the following:
3. Intrusion Detection/Prevention Systems (IDS/IPS)
4. Observation of suspicious behavior or unusual occurrences;
5. Lapses in physical or procedural security;
6. Information coming into the possession of unauthorized Personnel or Third Parties.
7. Information inappropriately exposed on a publicly facing website.
8. To assess whether a Security Event must be reported, Personnel should consider whether there are indications that:
9. Information was used by unauthorized Personnel or Third Parties;
10. Information has been downloaded or copied inappropriately from Vital College computer systems or equipment;
11. Equipment or devices containing Information have been lost or stolen;
12. Equipment or devices containing Information have been subject to unauthorized activity (e.g., hacking, malware).
13. Personal Data has been publicly exposed.
14. In addition, the following situations should be considered for Security Event reporting:
15. Ineffective security controls;
16. Breach of information integrity, confidentiality or availability expectations;
17. Human errors (innocent or otherwise);
18. Non–compliance with policies or standards;
19. Breaches of physical security arrangements;
20. Uncontrolled systems changes;
21. Malfunctions of software or hardware.
22. Access violations.
23. Even if Personnel are not sure whether a Security Event is an actual Security Incident, they are still required to report it as provided herein, as it is better to be cautious than to be compromised.
24. The SIRT will usually require the reporter to supply further information, which will depend upon the nature of the Security Event. However, the following information normally shall be supplied:
25. Contact name and information of the person reporting the Security Event.
26. Date and time the Security Event occurred or was noticed;
27. Type and circumstances of the Security Event;
28. The type of data, information, or equipment involved;
29. Location of the Security Event and data or equipment affected;
30. Whether the Security Event puts any person or other data at risk; and
31. Any associated ticket numbers, emails or log entries associated with the Security Event.
32. SIRT Primary Lead will ensure that the SIRT is promptly engaged once such notice is received. The following actions will also be taken:
33. The SIRT, under the leadership of the SIRT Primary Lead, shall use reasonable efforts to analyze the matter within four (4) hours of notice and decide whether to proceed with the Analysis Phase of the Incident Response Procedures.
34. Determination to initiate the Analysis Phase must be made quickly so that Personnel can make an initial determination as to the urgency and seriousness of the situation.
35. Upon making the decision to begin the Analysis Phase, if the SIRT suspects that the Security Event may result in damage to the reputation of Vital College or legal liability, the personnel responsible for Legal and Compliance shall initiate a legal assessment of actual or potential legal issues.

1. **Analysis Phase**

The initial response to the detection of a Security Event is typically the Analysis Phase. In this phase, the SIRT determines whether or not a Security Event is an actual Security Incident.

1. To determine if a Security Event is a Security Incident the following considerations apply:
2. Leverage diagnostic data to analyze the Security Event using tools directly on the operating system or application. This may include, but not be limited to:
3. Taking screenshots, memory dumps, consult logs and network traces.
4. Performing analysis on the information being collected.
5. Analyzing the precursors and indications.
6. Looking for correlating information; and
7. Performing research (e.g., search engines, knowledgebase).
8. Identify whether the Security Event was the result of an innocent error or the actions of a potential attacker. If the latter, effort shall be made to identify who the potential attacker may be, by:
9. Validating the attacker's IP address.
10. Researching the attacker through search engines.
11. Using incident databases.
12. Monitoring attacker communication channels, if possible; and
13. In unique cases, and with the approval of legal counsel, potentially scanning the attacker's system.
14. If the SIRT has determined that a Security Event has triggered a Security Incident, the appropriate SIRT team members will be engaged accordingly and the SIRT will begin documenting the investigation and gathering evidence. The type of Security Incident is based on the nature of the event. Example types are listed as follows:
15. Data exposure.
16. Unauthorized access.
17. Distributed Denial of Service/ Denial of Service (DDoS/DoS).
18. Malicious code.
19. Improper usage.
20. Scans/Probes/Attempted access.
21. If it is determined that a Security Incident has not been triggered, additional activities noted under 'Post-Incident Activities’ may be initiated under the direction of the SIRT.
22. The Security Incident’s potential impact on Vital College and/or its subscribers shall be evaluated and the SIRT shall assign an initial severity classification of low, medium, high, or serious/critical to the Security Incident. To analyze the situation, scope, and impact, the SIRT shall:
23. Define and confirm the severity level and potential impact of the Security Incident.
24. Identify which resources have been affected and forecast which resources will be affected.
25. Estimate the current and potential effect of the Security Incident.
26. The SIRT shall attempt to determine the scope of the Security Incident and verify if the Security Incident is still ongoing. Scoping the Security Incident may include collecting forensic data from suspect systems or gathering evidence that will support the investigation. It may also include identifying any potential data theft or destruction. New investigative leads may be generated as the collected data is analyzed. If the Security Incident involves malware, the SIRT shall analyze the malware to determine its capabilities and potential impact to the environment. Based on the evidence reviewed, the SIRT will determine if the Security Incident requires reclassification as to its severity or cause (e.g., whether it was originally thought to be the action of a malicious actor but turned out to be an innocent error or vice versa).
27. As indicated above, a Security Incident may require evidence to be collected. The collection of such evidence shall be done with due diligence and the following procedures shall apply:
28. Gathering and handling of evidence (forensics) should include:
29. Identifying information (e.g., the location, serial number, model number, hostname, media access control (MAC) address, and IP address of a computer);
30. Name, title, and phone number of everyone who collected or handled the evidence during the investigation.
31. Time and date (including time zone) of each occurrence of evidence handling.
32. Locations where the evidence was stored, and conditions of storage (e.g., locked spaces, surveilled spaces); and
33. Reasonable efforts to create two backups of the affected system(s) using new, unused media — one is to be sealed as evidence and one is to be used as a source of additional backups.
34. To ensure that evidence is not destroyed or removed, where any Personnel are suspected of being responsible for a Security Incident, Vital College shall, consistent with its procedures, use reasonable efforts to place monitoring and forensics agents and/or confiscate all computer/electronic assets that have been assigned to him or her.
35. This task may be done surreptitiously and should be completed as quickly and in as non-intrusive a manner as possible.
36. The SIRT should consider restricting access to the computers and attached peripherals (including remote access via modem, secure remote system access, etc.) pending the outcome of its examination.
37. Where applicable, and depending upon the seriousness of the Security Incident, items and areas that should be secured and preserved in an “as was” condition include:
38. Work areas (including wastebaskets);
39. Computer hardware (keyboard, mouse, monitor, CPU, etc.).
40. Software.
41. Storage media (disks, tapes, removable disk drives, CD ROMs, etc.);
42. Documentation (manuals, printouts, notebooks, notepads);
43. Additional components as deemed relevant (printer, cables, etc.);
44. In cases of damage, the computer system and its surrounding area, as well as other data storage devices, should be preserved for the potential collection of evidence (e.g., fingerprinting);
45. If the computer is “Off”, it should not be turned “On”. For a stand-alone computer system, if the computer is “On”, the Information Security and IT Departments are to be contacted.
46. It is important to establish who was using the computer system at the time of the Security Incident and/or who was in the immediate area. The SIRT should obtain copies of applicable records (e.g., access logs, swipe card logs, closed-circuit television recordings) as part of the investigation.
47. Based on the severity level and the categorization of the Security Incident, the proper team or Personnel shall be notified and contacted by the SIRT.
48. Until the SIRT, with the approval of Vital College management, makes the Security Incident known to other Personnel, the foregoing activities shall be kept confidential to the extent possible.
49. If it is determined that a Security Incident has occurred and may have a significant impact on Vital College or its subscribers, the SIRT shall determine whether additional resources are required to investigate and respond to the Security Incident. The extent of the additional resources will vary depending on the nature and significance of the Security Incident.

1. **Abnormal Activities Notification**

The SIRT recognizes that there may be many attempts to gain unauthorized access to, disrupt or misuse information systems and the information stored on them, and that many of these attempts will be thwarted by Vital College information security program. In general, the SIRT will not report unsuccessful attacks to customers. For example, the SIRT would generally not be required to report to a Data Controller or customer if it makes a good faith judgment that the unsuccessful attack was of a routine nature.

However, the SIRT will take reasonable steps to notify customers or Data Controllers of any identified Abnormal Activities. For example, in making a judgment as to whether a particular unsuccessful attack should be reported, Vital College might consider whether handling the attack required measures or resources well beyond those ordinarily used, like exceptional attention by senior personnel or the adoption of extraordinary non-routine precautionary steps. In cases of identified Abnormal Activities, the Data Controller or customer would be notified by means agreed upon by Vital College and the Data Controller or customer within twenty-four (24) hours upon Vital College becoming aware of the Abnormal Activity.

1. **Data Breach Notification**

If it is determined during the analysis phase that a Security Incident has occurred that constitutes a Data Breach, with notification obligations based on regulatory, legal, or similar requirements, notification of such Data Breach shall be provided to the impacted Data Controller by email, telephone, or other means agreed upon by Vital College and the Data Controller, within twenty-four (24) hours upon Vital College becoming aware of the Data Breach. Additional activities noted under ‘Post-Incident Activities’ may also be initiated under the direction of the SIRT.

1. **Containment Phase**

The Containment Phase mitigates the root cause of the Security Incident to prevent further damage or exposure. This phase attempts to limit the impact of a Security Incident prior to an eradication and recovery event. During this phase, the SIRT may implement controls, as necessary, to limit the damage from a Security Incident.

1. If a Security Incident is determined to be caused by innocent error, the eradication phase may not be needed. For example, after reviewing any information that has been collected investigating the Security Incident the SIRT may:
2. Secure the physical and network perimeter.
3. For example, shutting down a system, disconnecting it from the network, and/or disabling certain functions or services.
4. Connect through a trusted connection and retrieve any volatile data from the affected system.
5. Determine the relative integrity and the appropriateness of backing the system up.
6. If appropriate, back up the impacted system.
7. Change the password(s) to the affected system(s). Personnel, as appropriate, shall be notified of the password change.
8. Determine whether it is safe to continue operations with the affected system(s).
9. If it is safe, allow the system to continue to function, in which case the SIRT will:
10. Update the Incident Record; accordingly, and
11. Move to the Recovery Phase.
12. If it is not safe to allow the system to continue operations, the SIRT will discontinue the system(s) operation and move to Eradication Phase.
13. The SIRT may permit continued operation of the system under close supervision and monitoring if:
14. Such activity will assist in identifying individuals responsible for the Security Incident.
15. The system can run normally without risk of disruption, compromise of data, or serious damage; and
16. Consensus has been reached within the SIRT before taking the supervision and monitoring approach.
17. The final status of this stage should be appropriately documented in the Incident Record.
18. The SIRT shall apprise senior management of the progress, as appropriate.
19. During the Analysis and Containment Phases, the SIRT shall keep notes and use appropriate chain of custody procedures to ensure that the evidence gathered during the Security Incident can be used successfully during prosecution, if appropriate.

1. **Eradication Phase**

The Eradication Phase is the phase where vulnerabilities causing the Security Incident, and any associated compromises, are removed from the environment. An effective eradication for a targeted attack removes the attacker’s access to the environment all at once, during a coordinated containment and eradication event. Although the specific actions taken during the Eradication Phase can vary depending on the Security Incident, the standard process for the Eradication Phase shall be as follows:

1. Determine the symptoms and cause related to the affected system(s).
2. Eliminate components of the Security Incident. This may include deleting malware, disabling breached user accounts, etc.
3. Strengthen the controls surrounding the affected system(s), where possible (a risk assessment will be performed, if needed). This may include the following:
4. Strengthening network perimeter defences.
5. Improving monitoring capabilities or scope.
6. Remediating any security issues within the affected system(s), such as removing unused services or implementing general host hardening techniques.
7. Conduct a vulnerability assessment to verify that all the holes/gaps that can be exploited have been addressed
8. If additional issues or symptoms are identified, take appropriate preventative measures to eliminate or minimize potential future compromises.
9. Update the Incident Record with the information learned from the vulnerability assessment, including the cause, symptoms, and method used to fix the problem with the affected system(s).
10. If necessary, escalate to higher levels of support to enhance capabilities, resources, or time-to-eradication.
11. Apprise senior management of progress, as necessary.
12. After Vital College has implemented the changes for eradication, it is important to verify that cause of and individual(s) causing the Security Incident is fully eradicated from the environment. The SIRT shall also test the effectiveness of any security controls or changes that were made to the environment during containment and eradication.

1. **Recovery Phase**

The Recovery Phase represents the SIRT’s effort to restore the affected system(s) to operation after the problems that gave rise to the Security Incident, and the consequences of the Security Incident, have been corrected. Recovery events can be complex depending on the Security Incident type and can require full project management plans to be effective. Although the specific actions taken during the Recovery Phase can vary depending on the identified Security Incident, the standard process to accomplish this shall be as follows:

1. Execution of the following actions, as appropriate:
2. Installing patches.
3. Rebuilding systems.
4. Changing passwords.
5. Restoring systems from clean backups.
6. Replacing affected files with clean versions.
7. Determination whether the affected system(s) has been changed in any way.
8. If the system(s) has been changed, the system is restored to its proper, intended functioning (“last known good”).
9. Once restored, the system functions are validated to verify that the system/process functions as intended. This may require the involvement of the business unit that owns the affected system(s).
10. If operation of the system(s) had been interrupted (i.e., the system(s) had been taken offline), it should be restored and validated, and the system(s) should be monitored for proper behavior.
11. If the system(s) has not been changed in any way, but was taken offline (i.e., operations had been interrupted), restart the system and monitor for proper behavior.
12. Implementation of additional monitoring and alerting may be done to identify similar activities.
13. Update the Incident Record with any details determined to be relevant during this phase.
14. Apprise senior management of progress, as appropriate.

1. **Post Incident Activities Phase**

In addition to the Data Breach and Abnormal Activities notification requirements identified in the analysis phase above, and after verification of a successful containment and any necessary eradication, the SIRT shall take the following post-incident activities, as may be necessary:

1. Notification
2. When warranted or required by judicial action, law, or regulation, Vital College shall use reasonable efforts to provide notice to Personnel and/or affected parties about a Security Incident involving the Sensitive and/or Confidential Information of such stakeholders. For example:
3. Where it has been determined, or the SIRT and management reasonably believe, that there has been unauthorized access to or release of unencrypted customer data;
4. Where the Security Incident has compromised the security, confidentiality or integrity of Confidential Information.
5. Upon deciding to notify the SIRT, in consultation with senior management, shall use reasonable efforts to provide notice and disclosure to Personnel and/or affected parties within twenty-four (24) hours and, subject to applicable law, prior to notification of law enforcement personnel. Delay may nonetheless occur in instances where it is mandated or authorized by applicable law. For example, disclosure might be delayed if notice would impede a criminal investigation or if time is required to restore reasonable integrity to Vital College information systems.
6. The form and content of the of notification may be by letter or by email sent to an address where Personnel and/or affected parties can reasonably be expected to receive the disclosure or other, similar means.
7. The notification, in clear and plain language, may contain the following elements:
8. A description of the Security Incident that includes as much detail as is appropriate under the circumstances;
9. The type of information subject to unauthorized access;
10. Measures taken by Vital College to protect the Information of Personnel and/or affected parties from further unauthorized access;
11. A contact name and number that Personnel and/or affected parties may use to obtain further information;
12. Contact information for national credit reporting agencies;
13. Other elements as may be required by applicable law or whose inclusion the SIRT may otherwise consider appropriate under the circumstances.
14. Cooperation with external investigators
15. In the event that the SIRT considers it appropriate to inform law enforcement authorities or to retain forensic investigators or other external advisors, the following information shall be collected to provide to such authorities or investigators:
16. To the extent known, details of the:
17. Security Incident (date, time, place, duration, etc.);
18. Person(s) under suspicion (name, date of birth, address, occupation/position, employment contracts, etc.);
19. Computer and network log files pertaining to the Security Incident(s);
20. “Ownership” details of any Information that is allegedly stolen, altered, or destroyed;
21. The access rights to the computer system involved of the person(s) under investigation;
22. Information obtained from access control systems (e.g., computer logs, CCTV, swipe card systems, attendance logs, etc.); and
23. Any action taken by the IT department in relation to the computer systems concerned, including the date and time.
24. A copy of applicable Vital College Data Privacy and Security Policy (“Policy”) in force at the time of the incident (if applicable); and
25. Any other documentation or evidence relevant to the internal investigation of the Security Incident.
26. Information sharing
27. Security Incident-specific information (e.g., dates, accounts, programs, systems) must not be provided to any unknown individuals making such requests by telephone or email. Any release of Security Incident-specific information should only be to individuals previously identified by the SIRT. All requests for information from unknown individuals should be forwarded to the SIRT.
28. Contact with law enforcement authorities shall only be made by the Legal & Compliance in consultations with the SIRT and senior management.
29. In the event of a Security Incident, where members of the media make inquiries, Personnel are to be made aware that all requests for the release of information, press releases, or media interviews must be submitted to the DIRECTOR, and will only be released through the Vital College DIRECTOR or his or her appointed representative.
30. In consultation with the Legal & Compliance, SIRT and senior management, shall determine whether it is appropriate to issue a media statement, hold a press briefing, or schedule interviews.
31. If Sensitive and/or Confidential Information has been compromised and a significant number of individuals, as identified by the SIRT, are affected and/or suspected of being affected, Legal & Compliance, upon consultation with outside counsel and subject to applicable law, shall use reasonable efforts to contact applicable consumer reporting agencies prior to sending notices to the affected Personnel and/or affected parties.
32. Certain jurisdictions where Vital College does business, or where Vital College stakeholders reside, mandate different disclosure or notification obligations. Additionally, advice from both inside and outside counsel is required before communication occurs with credit reporting agencies.
33. Vital College will seek to ensure its obligations are fulfilled by quickly and professionally taking control of communication early during major events. Accordingly, Vital College will:
34. Designate a credible, trained, informed spokesperson to address the media;
35. Determine appropriate clearance and approval processes for the media;
36. Ensure the organization is accessible by media so they do not resort to other (less credible) sources for information;
37. Emphasize steps being taken to address the Security Incident;
38. Tell the story quickly, openly, and honestly to counter falsehoods, rumors, or undue suspicion.
39. When publicly disclosing information of a Security Incident, the following should be considered:
40. Was Personal Information compromised?
41. Was subscriber data compromised?
42. Were legal and/or contractual obligations invoked by the Security Incident?
43. What is the organization’s strategy moving forward?
44. Internal Communication
45. Where warranted, the SIRT will ensure that open communication is maintained within the organization to ensure relevant parties are informed of facts, reminded of responsibilities, and capable of dismissing rumors and speculation.
46. Aggregate documentation from post-mortem/follow-up reviews into the Security Incident record and create a formal report of the Security Incident to share with senior management, as necessary.

1. **Follow up Phase**

The Follow-up Phase represents the review of the Security Incident to look for “lessons learned” and to determine whether the process that was followed could have been improved in any way. Security Events and Security Incidents should be reviewed after identification resolution to determine where response could be improved.

1. The SIRT will meet to review the Security Event or Security Incident record created, as necessary, and perform the following:
2. Determine the root cause of the Security Incident and what should be done to ensure that the root cause has been addressed
3. Create a “lessons learned” document and include it with the Incident Record.
4. Evaluate the cost and impact of the Security Event or Incident to the organization using applicable documents and any other resources.
5. Determine what could be improved.
6. Communicate these findings to senior management for approval, as necessary, and for implementation of any recommendations made post-review of the Security Event or Incident.
7. Carry out recommendations approved by senior management while ensuring that sufficient time and resources are committed to this activity following the change management process.
8. Close the Security Event or Incident.

1. **Security Incident Records and Documentation**
2. The incident record should be verified during the follow-up process to ensure that it documents:
3. All relevant factual information or evidence;
4. Consultations with Personnel and external advisors; and
5. Findings resulting from the collection of factual information or evidence obtained.
6. The incident record shall be stored in electronic form in a central location.
7. Appropriate protections must be applied to guard against the alteration or deletion of the incident record.
8. Security Incident reports shall be kept for a minimum of 5 years.
9. **References**

|  |
| --- |
| **Document Name** |
|  |
|  |
|  |
|  |
|  |
|  |

1. **Outputs**

The following records need to be kept and stored securely.

|  |  |  |  |
| --- | --- | --- | --- |
| **Record** | **Responsible Person** | **Retention** | **Disposition** |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

All records must be stored in the pre-allocation location. All physical copies need to be stored in a lockable cabinet or drawer.

1. **Enforcement**

An employee found to have violated this procedure may be subject to disciplinary action, up to and including termination of employment. A violation of this procedure by a temporary worker, contractor or vendor may result in the termination of their contract or assignment with Vital College.

Any exception to the policy must comply with the **Exceptions Policy**.

1. **Definitions**

|  |  |
| --- | --- |
| **TERMS** | **DESCRIPTION** |
|  |  |

A black and white drawing of a handwritten note

Description automatically generated with low confidence

**DIRECTOR name** Duncan MacNicol **DIRECTOR signature**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**Signed at** Durban **on this** 20th day of February 2021

|  |  |  |
| --- | --- | --- |
|  | **Vital College (Pty) Ltd** | |
| Authorised by: | Duncan MacNicol |
| Date Authorised: | 20 February 2021 |
| Document Number: | VC-027 |



**Server Policy**

1. **Introduction**
   1. **Overview**

Unsecured and vulnerable servers continue to be a major entry point for malicious threats. Consistent Server installation policies, ownership and configuration management are all about doing the basics well.

* 1. **Scope**

All employees, contractors, consultants, temporary and other workers at Vital College and its subsidiaries must adhere to this policy. This policy applies to server equipment that is owned, operated, or leased by Vital College or registered under a Vital College owned internal network domain.

This policy specifies requirements for equipment on the corporate Vital College network.

The purpose of this policy is to establish standards for the base configuration of internal server equipment that is owned and/or operated by Vital College. Effective implementation of this policy will minimize unauthorized access to Vital College Confidential information and technology.

1. **Policy Statement**
   1. **General Requirements** 
      1. All internal servers deployed at Vital College must be owned by an operational group that is responsible for system administration. Approved server configuration guides must be established and maintained, based on business needs, and approved by IT and Security.
      2. The following items must be met:

Servers must be registered within the corporate enterprise management system. At a minimum, the following information is required to positively identify the point of contact:

* Server contact(s) and location, and a backup contact
* Hardware and Operating System/Version
* Main functions and applications, if applicable
* Information in the corporate enterprise management system must be kept up to date.
  + 1. For security, compliance, and maintenance purposes, authorized personnel may monitor and audit equipment, systems, processes, and network traffic.
  1. **Configuration Requirements**
     1. Operating System configuration should be in accordance with **Server Hardening Procedure**.
     2. Services and applications that will not be used must be disabled where practical.
     3. Access to services should be logged and/or protected through access-control methods such as a web application firewall, if possible.
     4. The most recent security patches must be installed on the system as soon as practical, the only exception being when immediate application would interfere with business requirements.
     5. Always use standard security principles of least required access to perform a function. Do not use root when a non-privileged account will do.
     6. Passwords for any systems installed on the Server needs to comply with the **Password Policy.**
     7. If a methodology for secure channel connection is available (i.e., technically feasible), privileged access must be performed over secure channels, (e.g., encrypted network connections using SSH or IPSec).
     8. Servers should be physically located in an access-controlled environment.
     9. Servers are specifically prohibited from operating from uncontrolled areas.
  2. **Monitoring**
     1. All security-related events on critical or sensitive systems must be logged and audit trails saved as follows:
* All security related logs will be kept online for a minimum of 1 week.
* Incremental backups will be retained for at least 1 month.
* Weekly full backups of logs will be retained for at least 1 month.
  + 1. Security-related events will be reported to InfoSec, who will review logs and report incidents to IT management. Corrective measures will be prescribed as needed. Security-related events include, but are not limited to:
* Port-scan attacks
* Evidence of unauthorized access to privileged accounts
* Anomalous occurrences that are not related to specific applications on the host.

**References**

|  |
| --- |
| **Document Name** |
| Server Hardening Procedure |
| Password Policy |
| Exceptions Policy |
|  |

**Outputs**

The following records need to be kept and stored securely.

|  |  |  |  |
| --- | --- | --- | --- |
| **Record** | **Responsible Person** | **Retention** | **Disposition** |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

All records must be stored in the pre-allocation location. All physical copies need to be stored in a lockable cabinet or drawer.

**Enforcement**

An employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment. A violation of this policy by a temporary worker, contractor or vendor may result in the termination of their contract or assignment with Vital College.

Any exception to the policy must comply with the **Exceptions Policy**.

**Definitions**

|  |  |
| --- | --- |
| **TERMS** | **DESCRIPTION** |
|  |  |

A black and white drawing of a handwritten note

Description automatically generated with low confidence

**DIRECTOR name** Duncan MacNicol **DIRECTOR signature**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**Signed at** Durban **on this** 20th day of February 2021



|  |  |  |
| --- | --- | --- |
|  | **Vital College (Pty) Ltd** | |
| Authorised by: | Duncan MacNicol |
| Date Authorised: | 20 February 2021 |
| Document Number: | VC-028 |

**Social Media Policy**

1. **Introduction**
   1. **Overview**

This policy provides guidance for employee use of social media, which should be broadly

understood for purposes of this policy to include blogs, wikis, microblogs, message boards, chat rooms, electronic newsletters, online forums, social networking sites, and other sites and services that permit users to share information with others in a contemporaneous manner.

* 1. **Responsibilities and Authorities**

Add the scope of the document

|  |  |  |
| --- | --- | --- |
| Role | Responsibility | Frequency |
| Administrator(s) | Will grant, deny or restrict access to any website, facility, and email size and network bandwidth and Regular review of logs generated from proxy server and mail server. | On-going/  Ad hoc |
| User | Shall identify themselves honestly, accurately and completely when corresponding or participating in interactive activities and shall not send unsolicited mass electronic mail. Will not impersonate any user.  Employees should not have any expectations of privacy as to his or her internet usage.  Employees are not allowed to change the internet settings set by Vital College. | On-going |
| CIO | Shall review this policy and make suggested and required amendments. | On-going |

1. **Policy Statement**

The following principles apply to professional use of social media on behalf of Vital College as well as personal use of social media when referencing Vital College.

* 1. Employees need to know and adhere to the Organisation’s Code of Conduct, and other company policies when using social media in reference to the organisation.
  2. Employees should be aware of the effect their actions may have on their images, as well as the organisation’s image. The information that employees post or publish may be public information for a long time.
  3. Employees should be aware that the organisation may observe content and information made available by employees through social media. Employees should use their best judgment in posting material that is neither inappropriate nor harmful to the organisation, its employees, or customers.
  4. Although not an exclusive list, some specific examples of prohibited social media conduct include posting commentary, content, or images that are defamatory, pornographic, proprietary, harassing, libelous, or that can create a hostile work environment.
  5. Employees are not to publish, post or release any information that is considered confidential or not public. If there are questions about what is considered confidential, employees should check with the Human Resources Department and/or supervisor.
  6. Social media networks, blogs and other types of online content sometimes generate press and media attention or legal questions. Employees should refer these inquiries to the authorized spokespersons.
  7. If employees encounter a situation while using social media that threatens to become antagonistic, employees should disengage from the dialogue in a polite manner and seek the advice of a supervisor.
  8. Employees should get appropriate permission before you refer to or post images of current or former employees, members, vendors or suppliers. Additionally, employees should get appropriate permission to use a third party's copyrights, copyrighted material, trademarks, service marks or other intellectual property.
  9. Social media use shouldn't interfere with employee’s responsibilities and computer systems are to be used for business purposes only. When using computer systems, use of social media for business purposes is allowed (ex: Facebook, Twitter, blogs, and LinkedIn), but personal use of social media networks or personal blogging of online content is discouraged and could result in disciplinary action.
  10. Subject to applicable law, after‐hours online activity that violates the Vital College Code of Conduct or any other company policy may subject an employee to disciplinary action or termination.
  11. If employees publish content after‐hours that involves work or subjects associated with the Vital College, a disclaimer should be used, such as this: “The postings on this site are my own and may not represent the Vital College positions, strategies or opinions.”
  12. It is highly recommended that employees keep the organisation’s related social media accounts separate from personal accounts, if practical.

**References**

|  |
| --- |
| **Document Name** |
| ISO/IEC 27001 standard, clauses A.13 |
|  |
|  |
|  |
|  |
|  |

**Outputs**

The following records need to be kept and stored securely.

|  |  |  |  |
| --- | --- | --- | --- |
| **Record** | **Responsible Person** | **Retention** | **Disposition** |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

All records must be stored in the pre-allocation location. All physical copies need to be stored in a lockable cabinet or drawer.

**Enforcement**

An employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment. A violation of this policy by a temporary worker, contractor or vendor may result in the termination of their contract or assignment with Vital College.

Any exception to the policy must comply with the **Exceptions Policy**.

**Definitions**

|  |  |
| --- | --- |
| **TERMS** | **DESCRIPTION** |
|  |  |

A black and white drawing of a handwritten note

Description automatically generated with low confidence

**DIRECTOR name** Duncan MacNicol **DIRECTOR signature**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**Signed at** Durban **on this** 20th day of February 2021



|  |  |  |
| --- | --- | --- |
|  | **Vital College (Pty) Ltd** | |
| Authorised by: | Duncan MacNicol |
| Date Authorised: | 20 February 2021 |
| Document Number: | VC-029 |

**Technology Disposal Policy**

1. **Introduction**
2. **Overview**

Technology equipment often contains parts which cannot simply be thrown away.  Proper disposal of equipment is both environmentally responsible and often required by law. In addition, hard drives, USB drives and other storage media contain various kinds of Vital College data, some of which is considered sensitive.  In order to protect our data, all storage mediums must be properly erased before being disposed of.  However, simply deleting or even formatting data is not considered sufficient.  When deleting files or formatting a device, data is marked for deletion, but is still accessible until being overwritten by a new file.  Therefore, special tools must be used to securely erase data prior to equipment disposal.

1. **Scope**

This policy applies to any computer/technology equipment or peripheral devices that are no longer needed within Vital College including, but not limited to the following: computers, servers, hard drives, laptops, portable storage devices (i.e., USB drives), backup tapes. For printed materials, please refer to the **Document Management Policy and Procedure**. This policy does not apply to Solid State Drives, when files are deleted from a solid-state drive, they are permanently deleted with no chance of data recovery.

The purpose of this policy it to define the guidelines for the disposal of technology equipment and components owned by Vital College (Pty) Ltd

1. **Policy Statement**
2. **Technology Equipment Disposal**
3. When Technology assets have reached the end of their useful life, they should be sent to the IT Team office for proper disposal.
4. The IT Team will securely erase all storage mediums.
5. All data including, all files and licensed software shall be removed from equipment using disk sanitizing software that cleans the media overwriting each and every disk sector of the machine with zero-filled blocks.
6. All electronic drives must be degaussed or overwritten with a commercially available disk cleaning program. Hard drives may also be removed and rendered unreadable (drilling, crushing or other demolition methods).
7. Technology equipment with non-functioning memory or storage technology will have the memory or storage device removed and the memory or storage will be physically destroyed.
8. **References**

|  |
| --- |
| **Document Name** |
| Document Management Policy and Procedure |
| Exceptions Policy |
|  |
|  |

1. **Outputs**

The following records need to be kept and stored securely.

|  |  |  |  |
| --- | --- | --- | --- |
| **Record** | **Responsible Person** | **Retention** | **Disposition** |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

All records must be stored in the pre-allocation location. All physical copies need to be stored in a lockable cabinet or drawer.

1. **Enforcement**

An employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment. A violation of this policy by a temporary worker, contractor or vendor may result in the termination of their contract or assignment with Vital College.

Any exception to the policy must comply with the **Exceptions Policy**.

1. **Definitions**

|  |  |
| --- | --- |
| **TERMS** | **DESCRIPTION** |
|  |  |

A black and white drawing of a handwritten note

Description automatically generated with low confidence

**DIRECTOR name** Duncan MacNicol **DIRECTOR signature**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**Signed at** Durban **on this** 20th day of February 2021



|  |  |  |
| --- | --- | --- |
|  | **Vital College (Pty) Ltd** | |
| Authorised by: | Duncan MacNicol |
| Date Authorised: | 20 February 2021 |
| Document Number: | VC-30 |

**Addendum to contract of employment**

**Protection of personal information act no.4 of 2013**

1. **Personal Information**
2. By submitting any personal information to the Company, the employee unconditionally and voluntarily, consents to the processing of the submitted personal information for any and all purposes related to employment agreement which may include, but is not limited to:
3. Collecting, organising, processing, and storing personal information for the business interests of the Company, as well as for the benefits of the employee and the Company;
4. Utilising personal information for screening, training and development, performance monitoring, career management, administration, employment relationship issues, termination of employment and any other employment-related purposes;
5. Sharing personal information with third parties, such as fund and insurance administrators and government departments. In certain circumstances personal information may be shared across borders when sharing the information with third parties.
6. Distributing relevant personal information when legally required to do so.
7. The parties agree to update, from time to time, any personal information supplied to each other, which may or has changed. The parties cannot be held liable for any loss caused by any of the parties’ failure to update and/or correct the personal information supplied to each other, by any of the parties.
8. The parties’ consent to the other party sharing the personal information (including but not limited to its group companies) for the purposes of this agreement and/or any other legitimate interests of the parties.
9. The employee is hereby informed that the personal information as shared with the Company may be transferred to a third party in order for the Company to fulfil its obligations under this agreement.
10. Should the employee’s personal information be shared cross border, the personal information will not be subject to less protection than it enjoys in terms of South Africa’s data privacy laws.

**Employee name**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ **Employee signature**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**Signed at** \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**on this** \_\_\_\_\_\_\_\_ **day of** \_\_\_\_\_\_\_\_\_\_\_**20**\_\_\_

**For and on behalf of**

**Employer name**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ **Employer signature**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**Witness name**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ **Witness signature**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_



|  |  |  |
| --- | --- | --- |
|  | **Vital College (Pty) Ltd** | |
| Authorised by: | Duncan MacNicol |
| Date Authorised: | 20 February 2021 |
| Document Number: | VC-031 |

**Addendum to the sub-contractor agreement**

**Protection of personal information act no.4 of 2013**

1. **Personal Information**
2. By submitting any personal information to the Company, the Sub-Contractor unconditionally and voluntarily, consents to the processing of the submitted personal information for any and all purposes related to employment agreement which may include, but is not limited to:
3. Collecting, organising, processing, and storing personal information for the business interests of the Company, as well as for the benefits of the Sub-Contractor and the Company;
4. Utilising personal information for screening, training and development, performance monitoring, career management, administration, Sub-Contractor relationship issues, termination of contract and any other contract-related purposes;
5. Sharing personal information with third parties, such as fund and insurance administrators and government departments. In certain circumstances personal information may be shared across borders when sharing the information with third parties.
6. Distributing relevant personal information when legally required to do so.
7. In order for the Company to fulfil its obligations in terms of the Sub-Contractor agreement.
8. The parties agrees to update, from time to time, any personal information supplied to each other, which may or has changed. The parties cannot be held liable for any loss caused by any of the parties failure to update and/or correct the personal information supplied to each other, by any of the parties.
9. The parties consent to the other party sharing the personal information (including but not limited to its group companies) for the purposes of this agreement and/or any other legitimate interests of the parties.
10. The Sub-Contractor is hereby informed that the personal information as shared with the Company may be transferred to a third party in order for the Company to fulfil its obligations under this agreement.
11. Should the Sub-Contractor’s personal information be shared cross border, the personal information will not be subject to less protection than it enjoys in terms of South Africa’s data privacy laws.

**Sub-Contractor name**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ **Sub-Contractor signature**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**Signed at** \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**on this** \_\_\_\_\_\_\_\_ **day of** \_\_\_\_\_\_\_\_\_\_\_**20**\_\_\_

**For and on behalf of**

**Company name**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ **Company signature**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**Witness name**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ **Witness signature**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

|  |  |  |
| --- | --- | --- |
|  | **Vital College (Pty) Ltd** | |
| Authorised by: | Duncan MacNicol |
| Date Authorised: | 20 February 2021 |
| Document Number: | VC-032 |



**Addendum to the independent contractor agreement**

**Protection of personal information act no.4 of 2013**

1. **Personal Information**
2. By submitting any personal information to the Company, the Independent Contractor unconditionally and voluntarily, consents to the processing of the submitted personal information for any and all purposes related to employment agreement which may include, but is not limited to:
3. Collecting, organising, processing, and storing personal information for the business interests of the Company, as well as for the benefits of the Independent Contractor and the Company;
4. Utilising personal information for screening, training and development, performance monitoring, career management, administration, Independent Contractor relationship issues, termination of contract and any other contract-related purposes;
5. Sharing personal information with third parties, such as fund and insurance administrators and government departments. In certain circumstances personal information may be shared across borders when sharing the information with third parties.
6. Distributing relevant personal information when legally required to do so.
7. In order for the Company to fulfil its obligations in terms of the Independent Contractor agreement.
8. The parties agrees to update, from time to time, any personal information supplied to each other, which may or has changed. The parties cannot be held liable for any loss caused by any of the parties failure to update and/or correct the personal information supplied to each other, by any of the parties.
9. The parties consent to the other party sharing the personal information (including but not limited to its group companies) for the purposes of this agreement and/or any other legitimate interests of the parties.
10. The Independent Contractor is hereby informed that the personal information as shared with the Company may be transferred to a third party in order for the Company to fulfil its obligations under this agreement.
11. Should the Independent Contractor’s personal information be shared cross border, the personal information will not be subject to less protection than it enjoys in terms of South Africa’s data privacy laws.

**Independent Contractor name**\_\_\_\_\_\_\_\_\_\_\_\_ **Independent Contractor signature**\_\_\_\_\_\_\_\_\_\_\_\_\_

**Signed at** \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**on this** \_\_\_\_\_\_\_\_ **day of** \_\_\_\_\_\_\_\_\_\_\_**20**\_\_\_

**For and on behalf of**

**Company name**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ **Company signature**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**Witness name**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ **Witness signature**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

|  |  |  |
| --- | --- | --- |
| C:\Users\JReddy\AppData\Local\Microsoft\Windows\INetCache\Content.Word\Vital small simple.jpg | **Vital College (Pty)Ltd** | |
| Authorised by: | Duncan MacNicol |
| Date Authorised: | 20 February 2021 |
| Document Number: | VC-033 |

**Addendum to the Internship agreement**

**Protection of personal information act no.4 of 2013**

1. **Personal Information**
2. By submitting any personal information to the Company, the Intern unconditionally and voluntarily, consents to the processing of the submitted personal information for any and all purposes related to employment agreement which may include, but is not limited to:
3. Collecting, organising, processing, and storing personal information for the business interests of the Company, as well as for the benefits of the Intern and the Company;
4. Utilising personal information for screening, training and development, performance monitoring, career management, administration, Internship relationship issues, termination of contract and any other contract-related purposes;
5. Sharing personal information with third parties, such as fund and insurance administrators and government departments. In certain circumstances personal information may be shared across borders when sharing the information with third parties.
6. Distributing relevant personal information when legally required to do so.
7. In order for the Company to fulfil its obligations in terms of the Internship agreement.
8. The parties agrees to update, from time to time, any personal information supplied to each other, which may or has changed. The parties cannot be held liable for any loss caused by any of the parties failure to update and/or correct the personal information supplied to each other, by any of the parties.
9. The parties consent to the other party sharing the personal information (including but not limited to its group companies) for the purposes of this agreement and/or any other legitimate interests of the parties.
10. The Intern is hereby informed that the personal information as shared with the Company may be transferred to a third party in order for the Company to fulfil its obligations under this agreement.
11. Should the Intern’s personal information be shared cross border, the personal information will not be subject to less protection than it enjoys in terms of South Africa’s data privacy laws.

**Intern name**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ **Intern signature**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**Signed at** \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**on this** \_\_\_\_\_\_\_\_ **day of** \_\_\_\_\_\_\_\_\_\_\_**20**\_\_\_

**For and on behalf of**

**Company name**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ **Company signature**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**Witness name**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ **Witness signature**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

|  |  |  |
| --- | --- | --- |
| C:\Users\JReddy\AppData\Local\Microsoft\Windows\INetCache\Content.Word\Vital small simple.jpg | **Vital College (Pty) Ltd** | |
| Authorised by: | Duncan MacNicol |
| Date Authorised: | 20 February 2021 |
| Document Number: | VC-034 |

**Addendum To Agreement Concluded Between**

**Insert Client Name**

(“The Client”)

And

**Vital College**

(“The Company”)

On**Insert Date**

(“The Agreement”).

1. **Introduction**

1. The provisions of this Addendum are to be read with the Agreement. Where provisions in this Addendum conflict with those in the Agreement, the provisions of this Addendum take precedence, unless agreed otherwise between the Parties.

1. **Data Protection**

1. This addendum will be applicable to all personal information as defined in the Protection of Personal Information Act, 4 of 2013 (“POPI”).
2. By either Party submitting any personal information to the other, the disclosing Party unconditionally and voluntarily, consents to the processing of the submitted personal information for any and all purposes related to this agreement.
3. The Parties agrees and consent that its personal information may be processed by, or on behalf of either of the Parties for the purposes set out in the Agreement.
4. The Parties shall at all times comply with its obligations and procure that each of its Affiliates comply with their obligations under POPI.

1. The Parties shall ensure that any personal information that is processed by it in the course of performing its obligations under the Agreement is done in accordance with POPI.

1. Each Party shall not process, disclose, or use personal information except:
2. to the extent necessary for the provision of Services and/or Products under the Agreement; or
3. to fulfil their own obligations under the Agreement; or
4. as otherwise expressly authorised by the other Party in writing.

1. Each Party shall not disclose any personal information to any Third Party without the other Party’s prior written consent in each instance, other than to the extent required by any Regulatoror Law.

1. In the event the other Party providing such consent necessary for the disclosure of personal information to a Third Party, each Party shall:
2. make such disclosure in compliance with POPI; and
3. enter into a written agreement with the applicable Third-Party recipient of such personal information that requires such Third Party to safeguard the personal information in a manner no less restrictive than each Party’s obligations under these terms.

1. The Parties shall implement and maintain an effective security safeguards that includes, but is not limited to administrative, technical, and physical safeguards, and appropriate technical and organisational measures, in each case, adequate to insure the security and confidentiality of personal information, and to protect against any anticipated risks to the security or integrity of personal information, protect against unauthorized access to or use of personal information,protect personal information against unlawful processing or processing otherwise than in accordance with this agreement, and protect against accidental loss, destruction, damage, alteration or disclosure of personal information.

1. Without limiting the foregoing, such safeguards and measures shall be appropriate to protect against the harm that may result from unauthorised or unlawful processing, use or disclosure, or accidental loss, destruction, or damage to or of Personal Information and the nature of the personal information, and shall maintain all safeguard measures as is required by POPI.

1. Each Party shall not use, process, store, transfer or permit access to any personal information across the borders of South Africa, without the written consent of the other Party.

1. In the event of any actual, suspected, or alleged security breach, including, but not limited to, loss, damage, destruction, theft, unauthorized use, access to or disclosure of any personal information, each Party shall:
2. notify the other Party as soon as practicable after becoming aware of such event.
3. provide the other Party will all information regarding the breach in the Party’s knowledge and possession to allow the Party to ascertain what has occurred and which personal information has been affected.
4. promptly take whatever action is necessary, at each Party’s own expense, to minimise the impact of such event and prevent such event from recurring.

**Client name**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ **Client signature**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**Signed at** \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**on this** \_\_\_\_\_\_\_\_ **day of** \_\_\_\_\_\_\_\_\_\_\_**20**\_\_\_

By the client who warrants their authority

**Company name**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**Company signature**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**Signed at** \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**on this** \_\_\_\_\_\_\_\_ **day of** \_\_\_\_\_\_\_\_\_\_\_**20**\_\_\_

By the company who warrants their authority



|  |  |  |
| --- | --- | --- |
|  | **Vital College (Pty) Ltd** | |
| Authorised by: | Duncan MacNicol |
| Date Authorised: | 20 February 2021 |
| Document Number: | VC-035 |

**Addendum to the Non-disclosure agreement**

**Protection of personal information act no.4 of 2013**

1. **Data Protection**

1. This addendum will be applicable to all personal information as defined in the Protection of Personal Information Act, 4 of 2013 (“POPI”).
2. By either Party submitting any personal information to the other, the disclosing Party unconditionally and voluntarily, consents to the processing of the submitted personal information for any and all purposes related to this agreement.
3. The Parties agrees and consent that its personal information may be processed by, or on behalf of either of the Parties for the purposes set out in the Agreement.
4. The Parties shall at all times comply with its obligations and procure that each of its Affiliates comply with their obligations under POPI.

1. The Parties shall ensure that any personal information that is processed by it in the course of performing its obligations under the Agreement is done in accordance with POPI.

1. Each Party shall not process, disclose or use personal information except:
2. to the extent necessary for the provision of Services and/or Products under the Agreement; or
3. to fulfil their own obligations under the Agreement; or
4. as otherwise expressly authorised by the other Party in writing.

1. Each Party shall not disclose any personal information to any Third Party without the other Party’s prior written consent in each instance, other than to the extent required by any Regulatoror Law.

1. In the event the other Party providing such consent necessary for the disclosure of personal information to a Third Party, each Party shall:
2. make such disclosure in compliance with POPI; and
3. enter into a written agreement with the applicable Third-Party recipient of such personal information that requires such Third Party to safeguard the personal information in a manner no less restrictive than each Party’s obligations under these terms.

1. The Parties shall implement and maintain an effective security safeguards that includes, but is not limited to administrative, technical, and physical safeguards, and appropriate technical and organisational measures, in each case, adequate to insure the security and confidentiality of personal information, and to protect against any anticipated risks to the security or integrity of personal information, protect against unauthorized access to or use of personal information,protect personal information against unlawful processing or processing otherwise than in accordance with this agreement, and protect against accidental loss, destruction, damage, alteration or disclosure of personal information.

1. Without limiting the foregoing, such safeguards and measures shall be appropriate to protect against the harm that may result from unauthorised or unlawful processing, use or disclosure, or accidental loss, destruction, or damage to or of Personal Information and the nature of the personal information, and shall maintain all safeguard measures as is required by POPI.

1. Each Party shall not use, process, store, transfer or permit access to any personal information across the borders of South Africa, without the written consent of the other Party.

1. In the event of any actual, suspected, or alleged security breach, including, but not limited to, loss, damage, destruction, theft, unauthorized use, access to or disclosure of any personal information, each Party shall:
2. notify the other Party as soon as practicable after becoming aware of such event;
3. provide the other Party will all information regarding the breach in the Party’s knowledge and possession to allow the Party to ascertain what has occurred and which personal information has been affected;
4. promptly take whatever action is necessary, at each Party’s own expense, to minimise the impact of such event and prevent such event from recurring.

**Disclosing Party**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ **Disclosing party signature**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**Signed at** \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**on this** \_\_\_\_\_\_\_\_ **day of** \_\_\_\_\_\_\_\_\_\_\_**20**\_\_\_

**Company name**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ **Company signature**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**Witness name**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ **Witness signature**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Where we refer to “process”, it means how we collect, use, store, make available, destroy, update, disclose, or otherwise deal with your personal information. As a general rule we will only process your personal information if this is required to deliver or offer a service, provide a product or carry out a transaction.

We may combine your personal information and use the combined personal information for any of the purposes stated in this Privacy Policy.

In this document any reference to “we” or “us” or “our” includes Our Company and any of its subsidiaries.

If you use our services, goods, products and service channels you agree that we may process your personal information as explained under this Privacy Policy. Sometimes you may provide us with consent to process your personal information. Read it carefully because it may limit your rights.

As a global organisation this Privacy Policy will apply to the processing of personal information by any member of our company globally. If we process personal information for another party under a contract or a mandate, the other party’s privacy policy will apply to the processing.

We can change this Privacy Policy from time to time if the law or its business practices requires it.

The version of the Privacy Policy displayed on our website will apply to your interactions with us.

**What is personal information?**

Personal information refers to any information that identifies you or specifically relates to you. Personal information includes, but is not limited to, the following information about you:

* your marital status (like married, single, divorced);
* your national origin;
* your age;
* your language; birth; education;
* your financial history (like your income, Third party payments made on your behalf and the like)
* your identifying number (like an employee number, identity number or passport number);
* your e-mail address; physical address (like residential address, work address or your physical location); telephone number;
* your biometric information (like fingerprints, your signature or voice);
* your race; gender; sex; pregnancy; ethnic origin; social origin; colour; sexual orientation;
* your physical health; mental health; well-being; disability; religion; belief; conscience; culture;
* your medical history (like your HIV / AIDS status); criminal history; employment history;
* your personal views, preferences and opinions;
* your confidential correspondence; and / or
* another’s views or opinions about you and your name also constitute your personal information.
* Personal information includes special personal information, as explained below.

**When will we process your personal information?**

We will only process your personal information for lawful purposes relating to our business if the following applies:

* if you have consented thereto;
* if a person legally authorised by you, the law or a court, has consented thereto;
* if it is necessary to conclude or perform under a contract we have with you;
* if the law requires or permits it;
* if it is required to protect or pursue your, our or a third party’s legitimate interest;

**What is special personal information?**

Special personal information is personal information about the following:

* your race (like where a company submits reports to the Department of Labour where the statistical information must be recorded);
* your ethnic origin;
* your trade union membership;
* your health (like where you apply for an insurance policy);
* your biometric information (like to verify your identity); and / or your criminal behaviour and alleged commission of an offence

**When will we process your special personal information?**

We may process your special personal information in the following circumstances:

* if you have consented to the processing;
* if the information is being used for any Human resource or payroll requirement;
* if the processing is needed to create, use or protect a right or obligation in law;
* if the processing is for statistical or research purposes and all legal conditions are met;
* if the special personal information was made public by you;
* if the processing is required by law;
* if racial information is processed, and the processing is required to identify you; and / or if health information is processed, and the processing is to determine your insurance risk, or to comply with an insurance policy or to enforce an insurance right or obligation.

**When and from where we obtain personal information about you**

* We collect personal information from the payroll or HR departments of our clients when they capture financial and non-financial information.
* We collect personal information from 3rd parties that are directly integrated with our software platform.
* We collect information about you based on your use of our products, services or service channels
* We collect information about you based on how you engage or interact with us such as via our support desk, emails, letters, telephone calls and surveys.

If the law requires us to do so, we will ask for your consent before collecting personal information about you from third parties.

The third parties from whom we may collect your personal information include, but are not limited to, the following:

* Partners of our company for any of the purposes identified in this Privacy Policy;
* your spouse, dependents, partners, employer, and other similar sources;
* people you have authorised to share your personal information, like a person that makes a travel booking on your behalf or a medical practitioner for insurance purposes;
* attorneys, tracing agents, debt collectors and other persons that assist with the enforcement of agreements;
* payment processing services providers, merchants, banks and other persons that assist with the processing of your payment instructions, like EFT transaction partners.
* insurers, brokers, other financial institutions or other organisations that assist with insurance and assurance underwriting, the providing of insurance and assurance policies and products, the assessment of insurance and assurance claims and other related purposes;
* law enforcement and fraud prevention agencies and other persons tasked with the prevention and prosecution of crime;
* regulatory authorities, industry ombudsman, governmental departments, local and international tax authorities;
* trustees, Executors or Curators appointed by a court of law;
* our service providers, agents and sub-contractors like couriers and other persons we use to offer and provide products and services to you;
* courts of law or tribunals;
* participating partners, whether retail or online, in our customer loyalty reward programmes;
* our joint venture partners; and / or

**Reasons we need to process your personal information**

* We will process your personal information for the following reasons:
  + to provide you with products, goods and services
  + to market our products, goods and services to you;
  + to respond to your enquiries and complaints;
  + to comply with legislative, regulatory, risk and compliance requirements (including directives, sanctions and rules), voluntary and involuntary codes of conduct and industry agreements or to fulfil reporting requirements and information requests;
  + to conduct market and behavioural research, including scoring and analysis to determine if you qualify for products and services or to determine your credit or insurance risk;
  + to develop, test and improve products and services for you;
  + for historical, statistical and research purposes, like market segmentation;
  + to process payment instruments .
  + to create, manufacture and print payment issues (like a payslip)
  + to enable us to deliver goods, documents or notices to you;
  + for security, identity verification and to check the accuracy of your personal information;
  + to communicate with you and carry out your instructions and requests;
  + for customer satisfaction surveys, promotional offerings.
  + insurance and assurance underwriting and administration;
  + to process or consider or assess insurance or assurance claims;
  + to provide insurance and assurance policies and products and related services;
  + to enable you to take part in customer loyalty reward programmes, to determine your qualification for participation, earning of reward points, determining your rewards level, monitoring your buying behaviour with our rewards partners to allocate the correct points or inform you of appropriate products, goods and services you may be interested in or to inform our reward partners about your purchasing behaviour;
  + to enable you to take part in and make use of value added products and services;
  + to assess our lending and insurance risks; and / or
  + for any other related purposes.

**How we use your personal information for marketing**

* We will use your personal information to market financial, insurance, investments and other related banking products and services to you.
* We may also market non-banking or non-financial products, goods or services to you.
* We will do this in person, by post, telephone, or electronic channels such as SMS, email and fax.
* If you are not our customer, or in any other instances where the law requires, we will only market to you by electronic communications with your consent.
* In all cases you can request us to stop sending marketing communications to you at any time.

**When, how and with whom we share your personal information**

In general, we will only share your personal information if any one or more of the following apply:

* if you have consented to this;
* if it is necessary to conclude or perform under a contract we have with you;
* if the law requires it; and / or
* if it’s necessary to protect or pursue your, our or a third party’s legitimate interests.

**Under what circumstances will we transfer your information to other countries?**

We will only transfer your personal information to third parties in another country in any one or more of the following circumstances:

* where your personal information will be adequately protected under the other country’s laws or an agreement with the third party recipient;
* where the transfer is necessary to enter into or perform under a contract with you, or a contract with a third party that is in your interest;
* where you have consented to the transfer; and / or
* where it is not reasonably practical to obtain your consent, the transfer is in your interest.

This transfer will happen within the requirements and safeguards of the law. Where possible, the party processing your personal information in the other country will agree to apply the same level of protection as available by law in your country or if the other country’s laws provide better protection the other country’s laws would be agreed to and applied.

An example of us transferring your personal information to another country is where foreign payments take place if you purchase goods or services in a foreign country.

**TAKE NOTE:** We are a global organisation your personal information may be shared within all our company entities in other countries and processed in those countries.

**Your duties and rights about the personal information we have about you**

* You must provide proof of identity when enforcing the rights below.

You must inform us when your personal information changes.

Please refer to our Promotion of Access to Information Act 2 of 2000 Manual (PAIA Manual) for further information on how you can give effect to the rights listed below. Download the PAIA Manual.

You have the right to request access to the personal information we have about you by contacting us. This includes requesting:

* confirmation that we hold your personal information;
* a copy or description of the record containing your personal information; and
* the identity or categories of third parties who have had access to your personal information.

We will attend to requests for access to personal information within a reasonable time. You may be required to pay a reasonable fee to receive copies or descriptions of records, or information about third parties. We will inform you of the fee before attending to your request.

Please note that the law may limit your right to access information.

You have the right to request us to correct or delete the personal information we have about you if it is inaccurate, irrelevant, excessive, out of date, incomplete, misleading, obtained unlawfully or we are no longer authorised to keep it. You must inform us of your request in writing. Please refer to our PAIA Manual for further information in this regard, like the process you should follow to give effect to this right. It may take up to 15 business days for the change to reflect on our systems. We may request documents from you to verify the change in personal information.

A specific agreement that you have entered into with us may determine how you must change your personal information provided at the time when you entered into the specific agreement. Please adhere to these requirements. If the law requires us to keep the personal information, it will not be deleted upon your request. The deletion of certain personal information may lead to the termination of your business relationship with us.

You may object on reasonable grounds to the processing of your personal information.

We will not be able to give effect to your objection if the processing of your personal information was and is permitted by law; you have provided consent to the processing and our processing done according to your consent or the processing is necessary to conclude or perform under a contract with you.

Where you have provided your consent for the processing of your personal information, you may withdraw your consent. If you withdraw your consent, we will explain the consequences to you. We may proceed to process your personal information even if you have withdrawn your consent if the law permits or requires it. It may take up to 15 business days for the change to reflect on our systems, during this time we may still process your personal information. You must inform us of any objection in writing. Please refer to our PAIA Manual for further information in this regard, like the process you should follow to give effect to this right.

You have a right to file a complaint with us or any Regulator with jurisdiction about an alleged contravention of the protection of your personal information by us. We will address your complaint as far as possible.

**How we secure your personal information**

* We will take appropriate and reasonable technical and organisational steps to protect your personal information according to industry best practices. Our security measures (including physical, technological and procedural safeguards) will be appropriate and reasonable. This includes the following:
* keeping our systems secure (like monitoring access and usage);
* storing our records securely;
* controlling the access to our buildings, systems and/or records; and
* safely destroying or deleting records.
* Ensure compliance with international ISO security standards.
* You can also protect your personal information. Please visit the website of the relevant business you have established a business relationship with for more information.

**How long do we keep your personal information?**

We will keep your personal information for as long as:

* the law requires us to keep it;
* a contract between you and us requires us to keep it;
* you have consented for us keeping it;
* we are required to keep it to achieve the purposes listed in this Privacy Policy;
* we require it for statistical or research purposes;
* a code of conduct requires us to keep it; and / or
* we require it for our lawful business purposes.

Take note: We may keep your personal information even if you no longer have a relationship with us, for the historical data that may be required by your employer or employee.

**Our cookie policy**

A cookie is a small piece of data sent from our websites or applications to your computer or device hard drive or Internet browser where it is saved. The cookie contains information to personalise your experience on our websites or applications and may improve your experience on the websites or applications. The cookie will also identify your device, like the computer or smart phone.

By using our websites or applications you agree that cookies may be forwarded from the relevant website or application to your computer or device. The cookie will enable us to know that you have visited the website or application before and will identify you. We may also use the cookie to prevent fraud and for analytics.



|  |  |  |
| --- | --- | --- |
|  | **Vital College (Pty) Ltd** | |
| Authorised by: | Duncan MacNicol |
| Date Authorised: | 20 February 2021 |
| Document Number: | VC-037 |

**Addendum To Agreement Concluded Between**

**Insert Supplier Name**

(“The Supplier”)

And

**Vital College**

(“The Company”)

On **Insert Date**

(“The Agreement”).

1. **Introduction**
2. The provisions of this Addendum are to be read with the Agreement. Where provisions in this Addendum conflict with those in the Agreement, the provisions of this Addendum take precedence, unless agreed otherwise between the Parties.

1. **Data Protection**
2. This addendum will be applicable to all personal information as defined in the Protection of Personal Information Act, 4 of 2013 (“POPI”).
3. By either Party submitting any personal information to the other, the disclosing Party unconditionally and voluntarily, consents to the processing of the submitted personal information for any and all purposes related to this agreement.
4. The Parties agrees and consent that its personal information may be processed by, or on behalf of either of the Parties for the purposes set out in the Agreement.
5. The Parties shall at all times comply with its obligations and procure that each of its Affiliates comply with their obligations under POPI.
6. The Parties shall ensure that any personal information that is processed by it in the course of performing its obligations under the Agreement is done in accordance with POPI.

1. Each Party shall not process, disclose or use personal information except:
2. to the extent necessary for the provision of Services and/or Products under the Agreement; or
3. to fulfil their own obligations under the Agreement; or
4. as otherwise expressly authorised by the other Party in writing.

1. Each Party shall not disclose any personal information to any Third Party without the other Party’s prior written consent in each instance, other than to the extent required by any Regulatoror Law.
2. In the event the other Party providing such consent necessary for the disclosure of personal information to a Third Party, each Party shall:
3. make such disclosure in compliance with POPI; and
4. enter into a written agreement with the applicable Third-Party recipient of such personal information that requires such Third Party to safeguard the personal information in a manner no less restrictive than each Party’s obligations under these terms.
5. The Parties shall implement and maintain an effective security safeguards that includes, but is not limited to administrative, technical, and physical safeguards, and appropriate technical and organisational measures, in each case, adequate to insure the security and confidentiality of personal information, and to protect against any anticipated risks to the security or integrity of personal information, protect against unauthorized access to or use of personal information,protect personal information against unlawful processing or processing otherwise than in accordance with this agreement, and protect against accidental loss, destruction, damage, alteration or disclosure of personal information.

1. Without limiting the foregoing, such safeguards and measures shall be appropriate to protect against the harm that may result from unauthorised or unlawful processing, use or disclosure, or accidental loss, destruction or damage to or of Personal Information and the nature of the personal information, and shall maintain all safeguard measures as is required by POPI.

1. Each Party shall not use, process, store, transfer or permit access to any personal information across the borders of South Africa, without the written consent of the other Party.

1. In the event of any actual, suspected or alleged security breach, including, but not limited to, loss, damage, destruction, theft, unauthorized use, access to or disclosure of any personal information, each Party shall:
2. notify the other Party as soon as practicable after becoming aware of such event;
3. provide the other Party will all information regarding the breach in the Party’s knowledge and possession to allow the Party to ascertain what has occurred and which personal information has been affected;
4. promptly take whatever action is necessary, at each Party’s own expense, to minimise the impact of such event and prevent such event from recurring.

**Supplier name**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ **Supplier signature**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**Signed at** \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**on this** \_\_\_\_\_\_\_\_ **day of** \_\_\_\_\_\_\_\_\_\_\_**20**\_\_\_

By the supplier who warrants their authority

**Company name**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**Company signature**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**Signed at** \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**on this** \_\_\_\_\_\_\_\_ **day of** \_\_\_\_\_\_\_\_\_\_\_**20**\_\_\_

By the company who warrants their authority