SEG INTERNATIONAL COLLEGE

Information Security Policy

Version – 1.2

Effective Date: December 22, 2022

Table of Contents

1 Introduction

“Information Security” refers to the processes and methodologies that SEG International College has designed and implemented to protect print, electronic, or any other form of confidential, private and sensitive information or data (“information”) from unauthorised access, acquisition, modification, misuse, disclosure, disruption or destruction. The purpose of this policy is to provide a security framework that will:

- Protect information and related assets from a range of threats.
- Maintain the confidentiality, integrity and availability of SEG International College, customer and business partner information and resources.
- Minimise business risks and maximise business opportunities related to information.

2 Who this Policy applies to

This policy applies to information assets owned or leased by SEG International College, and to devices that connect to the SEG International College network or reside at SEG International College sites. This policy applies to all staff, directors, contractors, temporary staff, consultants, volunteers and authorised agents of SEG International College.

For the purpose of this policy, the term ‘end user’ includes all groups who have access to SEG International College electronic resources.

The following mitigating controls are drawn from the Essential 8 Maturity Model developed by the Australian Cyber Security Centre (ACSC), as well as the National Institute of Standards and Technology (NIST) Cybersecurity Framework.

3 Information Security Policy

SEG International College handles sensitive information about students/Customers regularly that include their personal details, academic details and payment information. Sensitive Information must have adequate safeguards in place to protect them, to protect cardholder privacy, to ensure compliance with various regulations and to guard the future of the organization.

SEG International College commits to respecting the privacy of all its customers and to protecting any data about customers from outside parties. To this end management are committed to maintaining a secure environment in which to process customer information so that we can meet these promises.

Employees handling Sensitive data should ensure:

- Handle Company and student information in a manner that fits with their sensitivity.
- Limit personal use of SEG International College information and telecommunication systems and ensure it doesn’t interfere with your job performance.
- SEG International College reserves the right to monitor, access, review, audit, copy, store, or delete any electronic communications, equipment, systems, and network traffic for any purpose.
- Do not use e-mail, internet and other Company resources to engage in any action that is offensive, threatening, discriminatory, defamatory, slanderous, pornographic, obscene, harassing or illegal.
- Do not disclose personal information unless authorised.
- Protect sensitive customer information.
- Keep passwords and accounts secure.
- Do not install unauthorised software or hardware unless you have explicit management approval.
- Do not leave sensitive information in places that can be accessed by others, and do not leave computers unattended without locking the screen or logging off.
- Information security incidents must be reported, without delay, to the IT Administrator of the college.

4 Acceptable Use Policy

The Management's intentions for publishing an Acceptable Use Policy are not to impose restrictions that are contrary to SEG International College established culture of openness, trust and integrity. Management is committed to protecting the employees, partners and the Company from illegal or damaging actions by individuals, either knowingly or unknowingly.

- Employees are responsible for exercising good judgment regarding the reasonableness of personal use.
- Employees should ensure that they have appropriate credentials and are authenticated for the use of technologies.
- Employees should take all necessary steps to prevent unauthorized access to confidential data which includes student information.
- Employees should ensure that technologies should be used and setup in acceptable network locations.
- Keep passwords secure and do not share accounts.
- Authorized users are responsible for the security of their passwords and accounts.
- All PCs, laptops and workstations should be secured with a password protected screensaver with the automatic activation feature.
- Because information contained on portable computers is especially vulnerable, special care should be exercised.
- Postings by employees from a Company email address to newsgroups should contain a disclaimer stating that the opinions expressed are strictly their own and not necessarily those of SEG International College unless posting is in the course of business duties.
- Employees must use extreme caution when opening e-mail attachments received from unknown senders, which may contain viruses, e-mail bombs, or Trojan horse code.

5 Disciplinary Action

Violation of the standards, policies and procedures presented in this document by an employee will result in disciplinary action, from warnings or reprimands up to and including termination of employment. Claims of ignorance, good intentions or using poor judgment will not be used as excuses for non-compliance.

6 Protect Stored Data

- All sensitive Student data stored and handled by SEG International College, and its employees must be securely protected against unauthorized use at all times.

- Any sensitive data that is no longer required by SEG International College for business reasons must be discarded in a secure and irrecoverable manner.

- It is strictly prohibited to store Payment card information of the students on any media whatsoever.

7 Information Classification

Data and media containing data must always be labelled to include sensitivity level.

- **Confidential data** might include information assets for which there are legal requirements for preventing disclosure or financial penalties for disclosure, or data that would cause severe damage to SEG International College if disclosed or modified. Confidential data includes cardholder data.

- **Internal Use** data might include information that the data owner feels should be protected to prevent unauthorized disclosure.

- **Public data** is information that may be freely disseminated.

8 Access to Sensitive Payment Data

All access to student payment information should be controlled and authorised. Any job functions that require access to cardholder data should be clearly defined.

- Only Managing Director and Finance staff will have access to authorised payment services provider.

- Access rights to payment services provider should be restricted to lease privileges necessary to perform job responsibilities.

- No other employee should have access to payment services provider platform or access to any confidential data unless they have a genuine business need.

- SEG International College will ensure a written agreement that includes an acknowledgement is in place that the Service Provider will be responsible for the for the cardholder data that the Service Provider possess.

- SEG International College will ensure that a there is an established process including proper due diligence is in place before engaging with a Service provider.

- SEG International College will have a process in place to monitor the PCI DSS compliance status of the Service provider.

9 Physical Security

Access to sensitive information in both hard and soft media format must be physically restricted to prevent unauthorized individuals from obtaining sensitive data.

- Employees are responsible for exercising good judgment regarding the reasonableness of personal use.

- Employees should ensure that they have appropriate credentials and are authenticated for the use of technologies.

- Employees should take all necessary steps to prevent unauthorized access to confidential data.

- Employees should ensure that technologies should be used and setup in acceptable network locations.

- A “visitor” is defined as a vendor, guest of an employee, service personnel, or anyone who needs to enter the premises for a short duration, usually not more than one day.

- Keep passwords secure and do not share accounts. Authorized users are responsible for the security of their passwords and accounts.

- Media is defined as any printed or handwritten paper, received faxes, floppy disks, back-up tapes, computer hard drive, etc.

- Media containing sensitive information must be handled and distributed in a secure manner by trusted individuals.

- Visitors must always be escorted by a trusted employee when in areas that hold sensitive information.

- Procedures must be in place to help all personnel easily distinguish between employees and visitors, especially in areas where data is accessible. “Employee” refers to full-time and part-time employees, temporary employees and personnel, and consultants who are “resident” on SEG International College office.

- Strict control is maintained over the external or internal distribution of any media containing student data and has to be approved by management.

- Strict control is maintained over the storage and accessibility of media.

- All computer that store sensitive data must have a password protected screensaver enabled to prevent unauthorized use.

10 Protect Data in Transit

All sensitive data must be protected securely if it is to be transported physically or electronically.

- If there is a business justification to send student payment information or other sensitive information via email or via the internet or any other modes then it should be done after authorization and by using a strong encryption mechanism (i.e. – AES encryption, PGP encryption, IPSEC, GSM, GPRS, Wireless technologies etc.,).

- The transportation of media containing sensitive data to another location must be authorized by management, logged and inventoried before leaving the premises. Only secure courier services may be used for the transportation of such media. The status of the shipment should be monitored until it has been delivered to its new location.

11 Disposal of Stored Data

- All data must be securely disposed of when no longer required by SEG International College, regardless of the media or application type on which it is stored.

- An automatic process must exist to permanently delete on-line data, when no longer required.

- All hard copies of cardholder data must be manually destroyed as when no longer required for valid and justified business reasons. A quarterly process must be in place to confirm that all non-electronic cardholder data has been appropriately disposed of in a timely manner.

- SEG International College will have procedures for the destruction of hardcopy (paper) materials. These will require that all hardcopy materials are crosscut shredded, incinerated or pulped so they cannot be reconstructed.

- SEG International College will have documented procedures for the destruction of electronic media. These will require: – All data on electronic media must be rendered unrecoverable when deleted e.g. through degaussing or electronically wiped using military grade secure deletion processes or the physical destruction of the media; – If secure wipe programs are used, the process must define the industry accepted standards followed for secure deletion.

- All sensitive information awaiting destruction must be held in lockable storage containers clearly marked "To Be Shredded" - access to these containers must be restricted.

12 Security Awareness and Procedures

The Policies and procedures outlined below must be incorporated into company practice to maintain a high level of security awareness. The protection of sensitive data demands regular training of all employees and contractors.

- Review handling procedures for sensitive information and hold periodic security awareness meetings to incorporate these procedures into day-to-day company practice.

- Distribute this security policy document to all company employees to read. It is required that all employees confirm that they understand the content of this security policy document by signing an acknowledgement form.

- Company security policies must be reviewed annually and updated as needed.

13 System and Password Policy

All users, including contractors and vendors with access to SEG international College, systems, are responsible for taking the appropriate steps, as outlined below, to select and secure their passwords.

- A system configuration standard must be developed along industry acceptable hardening standards (SANS, NIST, ISO).

- System configurations must include common security parameter settings.

- All vendor default accounts and passwords for the systems have to be changed at the time of provisioning the system/device into network and all unnecessary services and user/system accounts have to be disabled.

- All unnecessary default accounts must be removed or disabled before installing a system on the network.

- Security parameter settings must me set appropriately on System components.

- All unnecessary functionality (scripts, drivers, features, subsystems, file systems, web servers etc.,) must be removed.

- All unnecessary services, protocols, daemons etc., should be disabled if not in use by the system

- Any insecure protocols, daemons, services in use must be documented and justified.

- All user must use a password to access the company network or any other electronic resources.

- All user ID's for terminated users must be deactivated or removed immediately.

- The User ID will be locked out if there are more than 5 unsuccessful attempts. This locked account can only be enabled by the system administrator. Locked out user accounts will be disabled for a minimum period of 30 minutes or until the administrator enables the account.

- All system and user level passwords must be changed on at least a quarterly basis.

- A unique password must be setup for new users and the users prompted to change the password on first login.

- The responsibility of selecting a password that is hard to guess generally falls to users.

- A strong password must:

    - Be as long as possible (never shorter than 8 characters).
    - Include mixed-case letters
    - Include digits and punctuation marks, if possible.
    - Not be based on any personal information.
    - Not be based on any dictionary word, in any language.

14 Anti-virus Policy

- All machines must be configured to run the latest anti-virus software as approved by SEG International College.

- The antivirus should have periodic scanning enabled for all the systems.

- The antivirus software in use should be cable of detecting all known types of malicious software (Viruses, Trojans, adware, spyware, worms and rootkits).

- All removable media (for example USB flash drive) should be scanned for viruses before being used. A

- Master Installations of the Antivirus software should be setup for automatic updates and periodic scans.

- End users must not be able to modify and any settings or alter the antivirus software.

- E-mail with attachments coming from suspicious or unknown sources should not be opened. All such e-mails and their attachments should be deleted from the mail system as well as from the trash bin. No one should forward any e-mail, which they suspect may contain virus.

- Employees are to contact college administrator to obtain the authorised anti-virus software and follow the above outlined guidelines.

15 Remote Access Policy

SEG International College provides flexibility to the employees to work remotely. Employees are to ensure the followings:

- It is the responsibility of all employees, contractors, vendors and agents with remote access privileges to SEG International College network and authorised platforms to ensure that their remote access connection is given the same consideration as the user's on-site connection to SEG International College

- Secure remote access must be strictly controlled.

- Remote access connection will be setup to be disconnected automatically after 30 minutes of inactivity.

- All hosts that are connected to SEG International College networks and authorised platforms via remote access technologies will be monitored on a regular basis.

16 Vulnerability Management Policy

- All the vulnerabilities would be assigned a risk ranking such as High, Medium and Low based on industry best practices such as CVSS base score.

- As part of PCI-DSS Compliance requirements, SEG International College will run internal and external network vulnerability scans at least quarterly and after any significant change in the network (such as new system component installations, changes in network topology, firewall rule modifications, product upgrades).

- Quarterly internal vulnerability scans must be performed by internal staff or a 3rd party vendor and the scan process have to include that rescans will be done until passing results are obtained, or all High vulnerabilities as defined in PCI DSS Requirement 6.2 are resolved.

17 Change Control Process

- 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, authorized, tested, implemented, and released in a controlled manner; and that the status of each proposed change is monitored.

- The change control process shall be formally defined and documented. A change control process shall be in place to control changes to all critical company information resources (such as hardware, software, system documentation and operating procedures). This documented process shall include management responsibilities and procedures. Wherever practicable, operational and application change control procedures should be integrated.

- All change requests shall be logged whether approved or rejected on a standardized and central system. The approval of all change requests and the results thereof shall be documented. A documented audit trail, maintained at a Business Unit Level, containing relevant information shall be maintained at all times. This should include change request documentation, change authorization and the outcome of the change. No single person should be able to effect changes to production information systems without the approval of other authorized personnel.

- A risk assessment shall be performed for all changes and dependent on the outcome, an impact assessment should be performed.

- The impact assessment shall include the potential effect on other information resources and potential cost implications. The impact assessment should, where applicable consider compliance with legislative requirements and standards.

- All change requests shall be prioritized in terms of benefits, urgency, effort required and potential impact on operations.

- 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. (For more information see System Development Life Cycle).

- Any software change and/or update shall be controlled with version control. Older versions shall be retained in accordance with corporate retention and storage management policies.

- 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.

- All users, significantly affected by a change, shall be notified of the change. The user representative shall sign-off on the change. Users shall be required to make submissions and comment prior to the acceptance of the change.

- Implementation will only be undertaken after appropriate testing and approval by stakeholders. All major changes shall be treated as new system implementation and shall be established as a project. Major changes will be classified according to effort required to develop and implement said changes.

- 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 back to what they were prior to implementation of changes.

- Information resources documentation shall be updated on the completion of each change and old documentation shall be archived or disposed of as per the documentation and data retention policies.

- 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.

- 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.