AIMS COLLEGE OF BUSINESS AND IT (PVT) LTD

IT POLICY

AIMS CAMPUS
TRANSFORMING LIVES

Introduction

Information is an asset to any organization, especially one focused on knowledge, such as AIMS, where information is used for learning and teaching, research, administration, and management. This policy addresses the administration and security of the institution's information, as well as its usage by its members and anyone who may lawfully process the institution’s information. All AIMS IT System users must read and understand the policy.

The overarching document of AIMS Information Security and Information Assurance Frameworks is the Data Protection Policy. This is meant to offer an overview of best practices in information security.

It should be read with the Frameworks' other rules and advice, some of which are beyond the scope of IT Services.

This and other Information Security Policies will be reviewed and updated on an annual basis, or in response to any substantial developments that may affect AIMS' overall security posture. All users shall be notified of such changes via the Intranet, direct communications, or both. When users are needed to use a new feature or modify their behavior, as is customary, supporting information will be supplied.

Purpose

The goal of this policy is to:

- Provide direction to university employees, students, and other users on the controls and assistance available to guarantee the security of the AIMS information and applications.
- To safeguard information technology assets and services of AIMS from unauthorized access, infiltration, interruption, or other harm.
- Maintaining the confidentiality, integrity, and availability of information utilized inside AIMS.
- To ensure compliance with applicable legislation and regulations, allowing AIMS to meet security standards such as Cyber Essentials (a security certification for organizations backed by the National Cyber Security Centre) and Payment Card Industry - Data Security Standards Compliance (PCI-DSS).

- To prevent the loss, disclosure, or corruption of personal information and intellectual property controlled by AIMS, its personnel, and students.

Scope

This policy applies to anybody who uses AIMS IT facilities (hardware, software, data, network access, third-party offered services, and other online services) that AIMS provides or arranges. It also applies to all information generated, received, or kept because of AIMS activity, which must be safeguarded based on its sensitivity, criticality, and worth, regardless of the medium or location in which the data is stored or accessible. AIMS Data Classification Policy contains information on sensitivity marking and information management.

Policy Statement

This policy is in place to prevent the danger of Information Security incidents interfering with the capacity of AIMS personnel, students, and other users to carry out their authorized operations. Awareness of what to do and what not to do to reduce those risks is also useful in assisting all of our users in being more aware of the Information Security concerns they encounter in their everyday life.

Responsibilities

The System Administrator is ultimately responsible for establishing information security at AIMS.

The System Administrator oversees and ensures that all information and information systems important to AIMS are effectively secured against the negative repercussions of information security breaches.

The System Administrator is obliged to execute this policy and is responsible for ensuring that employees, students, and other authorized individuals follow all related policies.

Individual users of AIMS IT equipment/services are responsible for complying with these and any associated rules, as well as reporting any policy violations, information security risks, or known vulnerabilities.

To aid understanding and use of this policy, it is divided into three duty areas:

- those of AIMS IT System users
- those of both users and providers of AIMS IT Systems
- those of AIMS IT System providers.

User Responsibilities

Handling Sensitive Information

Users of AIMS IT services will deal with a wide range of information, some of which will be sensitive. Although information may be labeled with its security classification, this is not always the case.

In such cases, the information should be considered Sensitive and appropriately handled if it contains

- Personal Information (PI) such as names, addresses, and performance observations
- Sensitive Personal Information (SPI), such as health records, political associations, sexuality, and criminal records;
- Potentially important commercial information, such as research and business plans
- Card Holder or bank data for persons or organizations
- User account credentials, including your own (user Identity and password)
- Configuration details for AIMS information Systems.

Employees who process Payment Card Data must read and understand the Payment Card Data Protection Policy. (under development)

Conduct

Users of AIMS IT services are required to behave reasonably, as described in the Acceptable Use Policy. (under development) The following are key features of anticipated behavior:

- You must not use AIMS IT equipment to cause unwarranted offense or distress to others, or to engage in actions that would violate legislation such as the Computer Misuse Act (1990), the Data Protection Act (2018), the Regulation of Investigatory Powers Act (2000), or AIMS Data Protection Policy.
- You are not permitted to send spam (unsolicited mass email).
- You must not create material or electronic communications that bring the institution into disrepute, offend, or otherwise harm its reputation. This includes using social media, both official AIMS profiles and personal accounts.
- You must not produce, download, view, store, or transmit illegal material, as well as indecent, offensive, defamatory, threatening, discriminatory, or extremist material. Any such behavior may be considered a criminal or civil offense and will be reported to the appropriate authorities.

Disciplinary Action

Violations of the standards, policies, and procedures outlined in this, and related publications may result in disciplinary action ranging from warnings or reprimands to termination of employment or removal from a course. Claims of ignorance, good intentions, or poor judgment will not be accepted as justifications for noncompliance.

Access to Sensitive Data

To secure sensitive data, AIMS has implemented access control systems. These give physical as well as logical controls. AIMS offers the bare minimum of access necessary for users to fulfill their tasks while also protecting sensitive data from unauthorized access. Users must follow the guidance provided in this and accompanying policies, particularly the Acceptable Use Policy and Payment Card Data Protection Policy - held by Finance (in production), if applicable to their job, and the Account Provisioning Policy, for these controls to be effective. (under development)

Data Loss Prevention

AIMS employ Data Loss Prevention (DLP) safeguards. The goal of these is to decrease the risk of unintentional or intentional disclosure, compromise, or loss of AIMS data assets, and it is part of AIMS’s efforts to satisfy Information Security requirements under DPA 2018 and GDPR. Additional improvements will be made through 2024.

These protections pertain to the disclosure or leaking of AIMS's most sensitive information, such as PI and SPI. These controls are now or will be implemented to services such as email, SharePoint, and Teams.

Users will be alerted if an activity they have performed or attempted has been discovered as a potential breach of DLP rules as a result of the modifications being implemented.

- Staff and students must be careful not to reveal personal information outside of AIMS network or to inside users who do not have the permission to read it. This might happen accidentally by forwarding an email to an external recipient or by declaring Microsoft Office 365 and AWS.
- Auto-forwarding of AIMS mailboxes is not permitted. As a result, critical information may leave the network. Consequently, when Auto Forward of emails is discovered, it will be disabled.

These actions are already being monitored, with notifications being provided to the Information Assurance and IT Security Teams.

Physical Security

The Physical Access Control Policy (under development) specifies the restrictions in place as well as the employees, students, and visitors' responsibilities for adhering to the policy.

• Staff and students should observe physical security controls and not allow "tailgating" through access-controlled doors and barriers;

• Wear their AIMS' passes at all times while on campus and/or present it virtually when requested to do so by AIMS staff

• Visitors must always be escorted by a trusted employee when entering areas containing sensitive (including cardholder) information and equipment

"Employee" refers to full-time and part-time workers, temporary employees, and other staff such as partners and examiners who are "resident" at AIMS facilities. A "visitor" is described as a vendor, an employee's guest, service staff, or anybody who must access the premises for a brief period of time, generally less than one day.

Employees must adhere to AIMS Clear Desk policy (under development) to avoid unauthorized access and loss of physical media and documentation.

Protection of Data in Transit

When transmitting sensitive data, it must be safeguarded with robust encryption. Payment card data has certain obligations, which will be outlined in the Payment Card Data Protection Policy (in preparation). Please see the Data Classification Policy (under development) for information on how to handle the four types of data: public, internal, confidential, and strictly confidential.

Disposal of Stored Data

When data is no longer needed, it must be safely disposed of, regardless of the medium or application type on which it is stored.

When a person or procedure marks online data for deletion, it must be permanently removed at that moment or after a specified retention period.

Data saved on media must be safely deleted using a certified and approved destruction technique.

Data hard copies must be safely destroyed by shredding. It is important to note that physical copies of credit card information must be destroyed by cross-cut shredding to certain specifications. They must not be placed in confidential trash containers to be shredded by a third party if done in the absence of AIMS workers responsible for data security. If available, further information can be found in the Payment Card Data Protection Policy.

Security Awareness and Procedures

To guarantee information security at AIMS, all users must be aware of this policy and those specified below. Supporting material is provided on the IT Services intranet website to help raise understanding of policy, processes, and guidelines. Prior to passing probation, all employees must complete the necessary IT Security training program (course) and must complete the IT security yearly refresher training.

System and Password Policy

When a new network password is established, Microsoft will evaluate its strength. Any password that is judged too weak or common will be denied and the user will be requested to provide an alternate.

- Be at least 8 characters long for staff and student IT accounts; admin accounts are designed to be longer.
- Include at least three of the following four-character types: upper and lower alpha, numeric, and special (symbols and punctuation).
- No dictionary terms or 'popular' passwords allowed.
- Do not include all or part of your username or any clear relationship to you, such as the name of a pet or a cousin.
- Be unique to your AIMS account and not be used for any other personal accounts.
- Should be adjusted as soon as the user or AIMS becomes aware of or thinks that an account has been hacked.
- Not to be revealed to anybody, even IT personnel. This includes never revealing MFA codes.
- Not be written down so that others can access them.

  Note. Passwords can be stored in a password management tool approved by IT Services.

- After 6 failed tries in a day, an account will be locked out; it may be reset using the Self-Service Password Reset (SSPR) service, but enrollment in SSPR is necessary first; click here to be directed to the SSPR service.
- Multi Factor Authentication (MFA) is in place for all Staff accounts while they are off site, and it has also been implemented for staff tech accounts when they are on site.
- Except for particularly controlled exceptions, MFA has been implemented for all student accounts.

During the COVID-19 Pandemic and the SL shutdown, the necessity for all employees and students to operate remotely was aided by a temporary waiver of the requirement to reset passwords every 90 days. This suspension has been reconsidered, and password aging is being reinstated.

Anti-Virus Policy

Malware protection will be enabled on all AIMS build devices. AIMS also includes email and online screening to limit the likelihood of consumers letting malware infect their devices.

Users cannot change the Anti-Virus software settings, which are intended to provide:

- Protection that is kept up to date with at least daily updates.
- Files are scanned upon access, and external media is automatically scanned when inserted into an AIMS device.
- Web sites are scanned before allowing access, and links included in emails are verified to be safe; those that are not flagged as suspect by internet providers and/or security services.

For PCI-DSS compliance, anti-virus product logs must be kept live for three months and archived for a 12-month record.

BYOD (Bring Your Own Device): When using a non-AIMS device for work, the user is responsible for ensuring that the same degree of AV protection is offered on their device.

It is not permitted to work on specific activities and projects when using a non-AIMS owned and controlled device. Devices used to process card payments or for the Babcock/MPS project are now included.

Patch Management Policy

The vendor must license and support any software used on devices and the network. When software is no longer supported, it must be deleted.

Wherever practical, all system software must have automatic updates enabled for vendor-released system fixes.

Patches for software and operating systems must be implemented within 30 days if the product vendor characterizes the patch as addressing a "critical" or "high risk" vulnerability. All security patches that are not labeled "critical" or "high risk" must be implemented within a month of their release.

Users assume the responsibilities outlined in this section while using their own devices. They must not utilize their own device for AIMS operations if they are unable to satisfy these patch management standards.

During important business times and when IT resources are constrained, AIMS implements change freezes. Patches and updates to operating systems and application software to address critical and high-risk security issues will continue to be applied to the above schedules during these freezes, unless there is good evidence that doing so would introduce a greater risk to service continuity or security than the security risk being addressed.

Use of Privileged Account

When utilizing a higher-privilege account, such as a technical account or domain admin account, you should be extra cautious about the hazards associated with the greater rights in case you are duped by an attacker. You must avoid utilizing these accounts for email or surfing unless you are working with a known supplier or doing a task that needs access to MS Azure. Higher privilege accounts must not have access to email or the internet, according to Cyber Essentials. As a result, such services should be used as little as possible.

Administration Access to a Device

AIMS provided laptop, tablets and desktop computers will allow user access to the functions of the device, but without the user having administrative privileges on the device. It will be possible for a user to be granted admin privileges to their device, but only for a specific purpose, for example the installation of approved software. The admin privileges will be revoked after a set period. Requests are currently made via a TOP desk ticket raised by the user. The process has been amended so that the user needs to provide a reason for the need for admin privileges and to identify how long the escalation is required, which will be limited to a week at most.

There will be exceptions to this regulation, such as when technicians in schools are responsible for managing the devices used in laboratories and lecturers require the capacity to install software pertinent to coursework.

All devices presently granted administrative rights must be evaluated and brought into compliance with the rules outlined above.

Secure Application Development

IT Services must authorize software used by AIMS for business reasons. All business-related goods must be offered by recognized and approved suppliers, with information security integrated in requirements and product specifications. As part of the Software Development Lifecycle (SDLC), evidence of Secure Application Development must be accessible.

User and AIMS's Joint Responsibilities

Remote Access Policy

Remote access for workers and students must be safeguarded so that no new security concerns are introduced.

For all off-site access, Multi Factor Authentication (MFA) is used to safeguard remote access. MFA is mostly accomplished via texting a PIN to a previously registered device or by using the Microsoft authenticator app. MFA is also used for AIMS on-site access by all admin accounts.

When personnel, students, contractors, suppliers, and agents no longer require remote access, it must be withdrawn. This will be done by the System Administrator who will disable or remove accounts as well as disable any remote access solutions given. For Cloud Service Partners who are no longer involved, this may need communication to third parties such as Microsoft and AWS.

Vulnerability Scanning and Management Policy

AIMS IT Services will conduct frequent internal and external network scans with recognized technologies. Using industry standards, these tools will determine the risk ranking.

PCI-DSS criteria will be satisfied, and the Payment Card Data Protection Policy will be outlined when it becomes available.

AIMS will execute scans on all new server and user device builds to ensure the security of the build before usage, as well as frequent network scans to discover vulnerabilities, even those thought to have been remediated following prior scans.

Configuration Standards

- AIMS IT Services will administer the Institution network to satisfy requirements
- Network devices will be configured to meet certain standards. These requirements shall be documented and reviewed and updated on a regular basis.
- Before being deployed to the network, network devices will be configured to fulfill these criteria.
- Automated configuration management solutions will be utilized whenever possible to maintain consistent configuration.

Change Control Process

AIMS IT Services has a Change Management mechanism in place. The Change Management Policy (under development) documents the Change Management process. Before being formally performed in the live environment, the procedure guarantees that all modifications are recorded, examined, authorized, and tested.

Within IT Services, a weekly BOM (Board of Management) meeting is held to ensure that any system modifications scheduled match the above-mentioned process standards and are either authorized or refused to proceed. BOM requests and approvals are kept on the Digital Transformations Project Committee on the website.

Audit and Log Review and Monitoring

AIMS retains the right, for any reason, to monitor, access, evaluate, audit, copy, store, or delete any electronic communications, equipment, systems, or network traffic within its domain.

User activity logs are stored and preserved, including logging in/out, access to programs, and Office 365 services. These logs are kept in order to fulfill regulatory and compliance obligations, although they are subject to retention schedules and deletion as part of routine cleaning.

Penetration Testing

AIMS will plan penetration testing of our systems in accordance with the security requirements required for PCI-DSS and Cyber Essentials (SLCERT–Sri Lanka Computer Emergency Readiness Team). This will be coordinated with third-party suppliers and carried out in such a way that it does not disrupt AIMS services' capacity or availability.

Joiners, Leavers and Movers

All accounts giving access to AIMS information systems are handled in accordance with the Account Provisioning Policy (under development) and through prescribed processes. These procedures encompass actions for Joiners, Leavers, and Movers, as well as access evaluations in the field. They include employees, contractors, researchers, and hourly paid lecturers. Students are also included.

Among the fundamental principles used are:

For all user categories, formal protocols are in place; access cannot be granted until initial verification and vetting (if necessary) are completed.

- Each user is assigned a unique User Identify and must have a Password that meets complex requirements.
- Each account offers the bare minimum of rights necessary for a user to carry out their duties.
- Additional access privileges must be requested in writing and implemented.
- Duties are separated to limit the possibility of misuse and fraud.
- Except for closely regulated exceptions approved by the Head of IT Security, group or shared accounts are not permitted.

For Information System operations, service accounts are permitted.

- Multi Factor Authentication will be required for any remote access.
- When on-site, those with greater rights and technical accounts are susceptible to MFA. Currently, a VPN is necessary for off-site remote access to particular 'high risk' apps.

All users must be aware of the Information Security Policy and associated rules in order to engage in responsible online behavior.

Wireless Policy

AIMS has wireless networks for both employees and students. These are separated in order to secure AIMS information.

Those processing Payment Card Transactions must NOT utilize the AIMS internal Wi-Fi service to process payments in order to comply with PCI-DSS.

Reporting

Any real or suspected violation of this policy should be promptly reported to IT Services. Any device that violates this policy can be presented to IT Services, which can rebuild the device to guarantee compliance with the policy.

Failure to Comply

Failure to comply with this policy or its subsidiary regulations may result in access to AIMS ICT Systems being revoked, as well as disciplinary action.

We appreciate your assistance in adhering to AIMS IT policy and procedures, as well as ensuring the safety and security of your device, our network, and services, as well as those of our partners and third-party providers. If you have any questions or need assistance, please contact the IT Services Service Desk or the IT Security team at dtpc@aimscollege.edu.lk .