Information Security Policy

1. Purpose and Scope

This Information Security Policy establishes the framework for protecting King's Own Institute's (KOI) information assets from unauthorised access, use, disclosure, disruption, modification, or destruction. This policy provides direction for managing information security in accordance with business requirements, relevant laws, and regulatory obligations.

The scope of this policy encompasses all information assets, systems, and technology infrastructure owned, managed, or operated by KOI, as well as all staff, students, contractors, visitors, and other authorised users who access KOI's information resources. It applies to all forms of information, including electronic data, physical documents, and verbal communications.

2. Related Documents

This Policy should be read in conjunction with KOI's:

- IT Disaster Recovery Policy
- IT Disaster Recovery Plan
- Provision and Acceptable Use of IT Resources Policy
- IT Strategy 2024-2026
- Bring Your Own Device (BYOD) Policy
- Privacy Policy

3. Definitions

Information Assets:	Any information or data owned or managed by KOI, regardless of format or medium, including electronic records, physical documents, and knowledge.
Information Security:	The protection of information and information systems from unauthorised access, use, disclosure, disruption, modification, or destruction to provide confidentiality, integrity, and availability.
Confidentiality:	Ensuring that information is accessible only to those authorised to have access.
Integrity:	Safeguarding the accuracy and completeness of information and processing methods.
Availability:	Ensuring that authorised users have access to information and associated assets when required.
Information Security Incident:	A suspected, attempted, successful, or imminent threat of unauthorised access, use, disclosure, breach, modification, or

	destruction of information; interference with information technology operations; or violation of this policy.
Risk Assessment:	The process of identifying, analysing, and evaluating risks associated with information assets.

4. Policy

4.1 Information Security Principles

KOI is committed to protecting its information assets by maintaining appropriate levels of confidentiality, integrity, and availability.

Information security management at KOI is governed by the following principles:

- KOI adopts a risk-based approach to information security, where security controls and resources are allocated based on risk assessment results, ensuring that high-risk areas receive appropriate attention. KOI implements a defence in depth strategy with multiple layers of security controls to provide redundant protection mechanisms.
- The principle of least privilege is enforced, whereby users are granted the minimum level of access necessary to perform their job functions. Critical functions are divided among different individuals to prevent fraud and error through segregation of duties.
- All information security practices comply with relevant legal, regulatory, and contractual requirements. KOI is committed to continuous improvement of information security controls and processes, which are regularly reviewed and enhanced in response to emerging threats, vulnerabilities, and business needs.

4.2 Information Classification

KOI information assets are classified into categories based on sensitivity and criticality:

- Public information is that which is intended for public disclosure or would have minimal impact if disclosed.
- Internal Use Only information is not intended for public disclosure but has limited sensitivity.
- Confidential information is sensitive and requires protection from unauthorised disclosure.
- Restricted information is highly sensitive that, if compromised, could cause significant damage to KOI, its stakeholders, or its operations.

Each classification level has associated handling requirements that govern how information should be stored, processed, transmitted, and disposed of. These requirements must be adhered to by all users handling KOI information assets.

4.3 Access Control

Access to KOI information assets is granted based on business need and is subject to strict controls. All users must have unique identifiers (user IDs) for access to KOI systems and applications. Authentication mechanisms appropriate to the classification of information being accessed must be implemented to ensure secure access.

Multi-factor authentication is required for accessing systems containing confidential or restricted information, particularly when accessed remotely. User access rights are reviewed regularly to ensure they remain appropriate to the user's role and responsibilities.

Access rights of users who change roles or leave KOI are adjusted or removed to prevent unauthorised access. The HR Manager must notify IT at least one week in advance of a staff member's resignation or transfer of role to ensure timely adjustment or removal of access rights. Privileged access rights are restricted, monitored, and reviewed more frequently than regular access rights due to their sensitivity.

The use of generic, shared, or service accounts must be strictly controlled and approved by the Director of IT. Such accounts present additional security risks and must be managed with appropriate compensating controls.

4.4 Information Security in System Development and Maintenance

Security requirements are identified and agreed upon before the development or implementation of new systems. This proactive approach ensures that security is built into systems from the beginning rather than added as an afterthought.

Secure coding practices are followed in all software development activities to prevent common vulnerabilities. Changes to systems are controlled through formal change management procedures to ensure that security is maintained throughout the system lifecycle.

Security testing is performed before systems are moved to production environments to identify and address vulnerabilities. Development, test, and production environments are separated to prevent unauthorised changes to production systems and data.

4.5 Physical and Environmental Security

Secure areas are protected by appropriate entry controls to ensure that only authorised personnel can access these areas. Equipment is protected from physical and environmental threats such as unauthorised access, theft, fire, water damage, and power failures.

Power supplies, telecommunications cabling, and other utilities are protected from interception, interference, and damage to maintain the confidentiality, integrity, and availability of information. Equipment maintenance is carried out in accordance with manufacturer recommendations to ensure continued availability and integrity.

Information-bearing equipment or media is not removed from KOI premises without prior authorisation to prevent data loss or theft. This includes laptops, mobile devices, USB drives, and other portable storage media containing KOI information.

4.6 Operations Security

Operating procedures are documented and made available to all users who need them to ensure consistent and secure operation of information processing facilities. Changes to operational systems and applications are controlled to minimise the risk of security incidents.

System capacity is monitored and future requirements projected to ensure adequate resources are

available when needed. Development, testing, and operational environments are separated to reduce the risk of unauthorised access or changes to operational systems.

Controls against malware are implemented and regularly updated to protect against security threats. Regular backups of information, software, and system configurations are performed and tested to ensure that they can be restored when needed.

Technical vulnerabilities are identified, evaluated, and remediated in a timely manner to prevent exploitation. This includes regular vulnerability scanning, patch management, and security updates.

4.7 Communications Security

Networks are managed and controlled to protect information in systems and applications. Security mechanisms, service levels, and management requirements for all network services are identified and included in network service agreements.

Information transferred through networks is protected from interception, copying, modification, misrouting, and destruction through appropriate security controls. Formal transfer policies, procedures, and controls are in place to protect the transfer of information through the use of all types of communication facilities.

4.8 Incident Management

All information security incidents or suspected incidents must be reported promptly to the IT Service Desk. Timely reporting allows for rapid response and containment of security breaches.

Responsibilities and procedures for managing information security incidents are established to ensure effective and consistent handling. Information gained from the assessment and resolution of information security incidents is used to identify recurring or high-impact incidents and improve security controls.

Evidence related to information security incidents is collected, retained, and presented in accordance with legal requirements. This ensures that KOI can take appropriate legal action if necessary and learn from incidents to prevent future occurrences.

4.9 Business Continuity Management

Information security continuity is embedded within the organisation's business continuity management systems. This ensures that information security is maintained during disruptive events.

Procedures are established to ensure the required level of information security during disruptive events. These procedures are tested regularly to verify their effectiveness.

Redundancy of information processing facilities is implemented where required to meet availability requirements. This includes backup systems, alternative processing sites, and redundant network connections.

4.10 Compliance

All relevant legislative, regulatory, and contractual requirements are explicitly identified,

documented, and kept up to date. This ensures that KOI remains compliant with all applicable laws and regulations.

Appropriate procedures are implemented to ensure compliance with these requirements. Information systems are regularly reviewed for technical compliance with security policies and standards.

Regular audits of information security controls are conducted to verify their effectiveness and compliance with this policy. Audit findings are addressed promptly to maintain an effective information security posture.

4.11 Cybersecurity and Threat Protection

Advanced security controls are implemented to protect against sophisticated cyber threats. These include intrusion prevention systems, endpoint protection, and data loss prevention tools.

Security monitoring systems are deployed to detect and respond to security events in real-time. This enables rapid identification and containment of security incidents.

Threat intelligence is collected and analysed to identify emerging threats to KOI's information assets. This proactive approach allows KOI to implement countermeasures before threats materialise.

Security awareness training is provided to all users to help them identify and respond to social engineering attacks. This training is updated regularly to address emerging threats.

Regular security assessments and penetration testing are conducted to identify and address vulnerabilities. This helps ensure that KOI's security controls remain effective against evolving threats.

Artificial Intelligence and Machine Learning technologies, including Generative AI, must be used in accordance with the Provision and Acceptable Use of IT Resources Policy and Use of Artificial Intelligence Policy. This ensures that these technologies do not introduce new security risks.

5. Roles and Responsibilities

5.1 AIBM Council

The AIBM Council approves the Information Security Policy and ensures that information security is aligned with KOI's strategic objectives. It provides oversight of information security risk management and ensures that appropriate resources are allocated to maintain an effective information security program.

5.2 Audit and Risk Committee

The Audit and Risk Committee reviews and recommends approval of the Information Security Policy to the AIBM Council. It monitors compliance with the policy and reviews major information security incidents and risk assessments to ensure that appropriate actions are taken.

5.3 Director of IT

The Director of IT owns and maintains the Information Security Policy and is responsible for developing and implementing information security procedures and guidelines. The Director monitors

and reports on information security compliance, coordinates information security incident response, and provides regular reports to the CEO/President and AIBM Council regarding information security status.

5.4 IT Reference Group (ITRG)

The IT Reference Group provides input on information security requirements and controls based on business needs. It reviews and provides feedback on information security policies and procedures and assists with information security risk assessments to ensure that security controls are aligned with business objectives.

5.5 System Owners

System Owners ensure that information security controls are implemented in their systems in accordance with this policy. They conduct regular risk assessments of their systems, approve access to their systems based on business need, and report security incidents affecting their systems to the IT Service Desk.

5.6 All Users

All users must comply with the Information Security Policy and related procedures. They are responsible for protecting information assets under their control, reporting information security incidents or vulnerabilities, attending information security awareness training, and using information assets only for authorised purposes.

6. Implementation and Compliance

6.1 Implementation

This policy is implemented through the development and implementation of information security procedures and guidelines. Regular information security awareness training is provided for all users to ensure they understand their responsibilities.

Technical security controls are implemented across KOI's IT infrastructure to enforce the policy requirements. Regular security assessments and audits are conducted to verify compliance and identify areas for improvement.

Information security incident management procedures are established to ensure consistent and effective handling of security incidents. These procedures are tested regularly to verify their effectiveness.

6.2 Non-Compliance

Non-compliance with this policy may result in disciplinary action. For students, this may include disciplinary action under the Student Non-Academic Misconduct Policy. For staff, disciplinary action may be taken under the Staff Code of Conduct.

For contractors and third parties, non-compliance may result in termination of contracts or service agreements. For all users, restriction or revocation of access to KOI's information systems and resources may be imposed to protect KOI's information assets.

7. Review and Maintenance

This policy will be reviewed annually, or more frequently if required due to changes in technology, threats, business requirements, or legislation. The Director of IT is responsible for initiating and coordinating the review process to ensure that the policy remains current and effective.

Document Control

Policy title	**Information Security Policy**
Policy owner	Director of Information Technology
Policy version date	13 June 2025
Policy approver	AIBM Council
Date of approval	13 June 2025
Date of implementation	13 June 2025
Date of next review	13 June 2026
Changes in this version	New Policy