Information Systems Management Policy and Protocols

Version	Approved by	Approval date	Review date
01	Board of Directors	August 2024	September 2025

Administrators Responsible	President, IT Manager
Purpose	The purpose of the Information Systems Management Policy and Protocols (ISMP) document is to establish guidelines for the management, operation, and security of information systems. This policy aims to ensure the integrity, availability and confidentiality of ISGL's information assets.
Scope	This policy applies to all students, faculty, staff, contractors, and any individuals who access, use, or manage ISGL's information systems and data.

1. INFORMATION SYSTEMS MANAGEMENT

The management of information systems is a critical component of our commitment to ensuring the integrity, security and availability of our information assets. This section elaborates on the core principles and protocols governing the management of ISGL's information systems.

a. System Ownership

i. Responsibilities: Each information system at ISGL must have a designated System Owner. This individual is responsible for the overall management and security of the system. Their responsibilities include ensuring proper access controls are in place, data is classified and handled according to its sensitivity, and the system complies with all relevant policies and legal requirements.

ii. Accountability: System Owners are accountable for conducting regular reviews of the system's security posture, approving access requests, and overseeing the system's operation to ensure it meets ISGL's strategic objectives.

b. Access Control

i. Principle of Least Privilege: Access to information systems shall be limited to what is strictly required for users to fulfill their job duties. Unnecessary access rights shall be avoided to minimise potential avenues for data breach or system compromise.

ii. Need-to-Know Basis: Access decisions shall also be made based on the 'need-to-know' principle, where users are given access only to the information necessary for their role.

iii. Authentication and Authorisation: Robust authentication mechanisms must be employed. This includes strong password policies, periodic password changes, and where appropriate, multi-factor authentication. Authorisation processes must ensure users are granted access for appropriate durations without exceeding their role requirements.

c. Data Classification and Handling

i. Data Classification: Information within ISGL's systems will be classified into categories (e.g., Public, Internal, Confidential, Highly Confidential) based on sensitivity and impact of disclosure. This classification guides the handling, transmission, and storage of data.

ii. Handling Protocols: Data handling protocols will dictate measures for encryption, storage, and transmission of data, ensuring that sensitive information is adequately protected both at rest and in transit. Special attention will be given to personal and sensitive personal data to comply with privacy laws and regulations.

d. System Development and Acquisition

i. Security by Design: New systems development and acquisition processes must incorporate security considerations from the outset, following the principle of 'security by design'. This includes conducting risk assessments, privacy impact assessments, and ensuring systems are capable of implementing necessary security controls.

ii. Compliance and Standards: All new systems or major updates must comply with ISGL's established IT and security standards, as well as relevant legal and regulatory requirements. System acquisition procedures must include security criteria in vendor selection and contract agreements.

2. INFORMATION SECURITY

ISGL is dedicated to maintaining the highest level of information security across all its information systems. This commitment is critical to protecting our community's data and ensuring the trustworthiness and reliability of our academic and administrative operations. The following protocols detail our approach to achieving and sustaining this goal.

a. User Authentication

i. Secure Authentication Methods: ISGL requires all users to be authenticated using secure and robust methods to access its information systems. This includes, but is not limited to, strong password policies that require a mix of letters, numbers, and special characters, as well as regular password updates.

ii. Multi-Factor Authentication (MFA): For systems that contain sensitive or critical information, ISGL implements multi-factor authentication. MFA requires users to verify their identity using at least two forms of credentials beyond just a password, such as a code from a smartphone app or a fingerprint. This significantly enhances security by mitigating the risk of unauthorised access resulting from compromised passwords.

iii. Authentication Protocols Review: ISGL regularly reviews and updates its authentication protocols to adapt to new security challenges and technological advancements.

b. Malware Protection

i. Antivirus Software: All devices that access ISGL's information systems must be equipped with up-to-date antivirus software. This software is essential for detecting, quarantining and removing malicious software to prevent harm to ISGL's systems and data.

ii. Regular Updates and Scans: ISGL ensures that antivirus software on all devices is kept up-to-date with the latest malware definitions and security patches. Regular scans are performed to identify and mitigate potential threats promptly.

iii. Device Compliance: Devices that do not meet ISGL's malware protection standards are restricted from accessing the network until compliance is achieved, safeguarding against potential security breaches.

c. Information Security Incidents

i. Incident Reporting: ISGL mandates the immediate reporting of all suspected or actual security incidents to the IT Department. This includes any unauthorised access, data breaches, loss of data, or malware infections.

ii. Investigation and Response: The IT Department, in collaboration with relevant stakeholders, will investigate reported incidents to ascertain their impact and coordinate an effective response. This may involve system isolation, data recovery, and legal action, as necessary.

iii. Documentation and Learning: All security incidents are documented in a Security Incident Register. This register is reviewed regularly to identify patterns and areas for improvement. Lessons learned from incidents are incorporated into ISGL's security strategies and shared with relevant parties to prevent recurrence.

d. Security Awareness Training

i. Regular Training Programs: ISGL commits to providing regular security awareness training for all individuals who use its information systems. This training covers topics such as safe internet practices, recognising phishing attempts, securing personal and ISGL data and reporting security incidents.

ii. Customized Content: Training content is tailored to the specific roles and responsibilities of different user groups within ISGL, ensuring relevance and effectiveness.

iii. Continuous Learning: Security awareness is an ongoing process. As such, ISGL fosters a culture of continuous learning and vigilance against new and evolving cyber threats. Regular updates, newsletters, and security alerts are provided to the ISGL community to maintain high levels of awareness.

3. MAINTENANCE AND MONITORING

ISGL recognises the critical importance of the regular maintenance and diligent monitoring of its information systems to uphold security standards and ensure system availability. This section outlines the protocols for systematic system maintenance and rigorous monitoring and logging practices.

a. System Maintenance

i. Scheduled Maintenance: ISGL commits to performing routine and scheduled maintenance on all information systems. This maintenance is essential for ensuring the systems operate efficiently, securely and are available when needed by the ISGL community.

ii. Security Patches: A key component of system maintenance is the application of security patches. These patches address vulnerabilities within systems that could be exploited by cyber threats. ISGL prioritises the timely application of these patches to mitigate potential security risks.

iii. System Audits: Regular system audits are conducted to review and assess the security posture of ISGL's information systems. These audits help identify any security weaknesses or compliance issues, allowing for prompt corrective actions.

iv. Maintenance Notifications: To minimise disruption, ISGL provides advance notice of scheduled maintenance activities to all affected users. These notifications include the date, time and expected duration of maintenance, as well as any anticipated impacts on system availability.

v. Record Keeping: Detailed records of all maintenance activities, including the application of security patches and outcomes of system audits, are maintained. These records are essential for historical analysis, compliance verification, and planning future maintenance activities.

b. Monitoring and Logging

i. Continuous Monitoring: ISGL employs continuous monitoring strategies to oversee the operation and security of its information systems. This proactive approach allows for the early detection of potential security incidents, system malfunctions, or unauthorised activities.

ii. Access Logging: All access to ISGL's information systems is logged, including user identification, time of access and the specific resources accessed. These logs play a crucial role in investigating security incidents and ensuring user accountability.

iii. Anomaly Detection: Automated tools are utilised to analyse log data and identify anomalies or patterns indicative of unauthorised or suspicious activities. Upon detection, alerts are generated for further investigation by the IT Department.

iv. Incident Investigation: In the event of a suspected security incident, the detailed logs serve as a critical resource for the IT Department to trace actions, determine the scope of the incident, and identify the involved parties.

4. POLICY REVIEW AND UPDATE

This policy will be reviewed annually and updated as necessary to reflect changes in technology, legal requirements, and organisational priorities.

Related Documents

a. Critical Incident Policy
b. IT Security Measures and Procedures
c. Privacy Policy
d. Staff Code of Conduct