S

| | | | | |
|---|---|---|---|---|
| AIU AMERICAN INTERNATIONAL UNIVERSITY الجامعة الأمريكية الدولية | Policy Main Title | Information Systems and Technology Governance Policy | Effective Date | 14/06/2026 |
| | Category | Academic | Last Review date | |
| | Policy Number | ADM-004 | Next Review date | 14/06/2029 |
| | Responsible Entity | Chief Information Officer | Approved By | President |

**Overview**

Information systems and technology are foundational to AIU's educational mission. The Learning Management System (Canvas) delivers course content and assessment. The Student Information System (Banner) maintains academic records and enrolment data. Institutional research platforms generate the student outcome data required by Accreditation agency. Email, collaboration tools, and digital databases support teaching, research, and administration. Without reliable, secure, and well-governed information systems, AIU cannot deliver its programs, assess student learning, or demonstrate institutional effectiveness to its accreditor.

Accreditation agency requires that technology resources be sufficient in scope, quality, currency, and kind to support the educational objectives of the institution. This standard is evaluated not only by asking whether systems exist but whether they are reliably available, properly secured, and actively managed. An institution whose LMS is frequently unavailable, whose student data is not backed up, or whose faculty have no IT support during examination periods has not satisfied the requirement, regardless of how sophisticated its technology appears on paper.

This policy establishes the governance framework for all information systems and technology at AIU. It defines how technology decisions are made and resourced, how institutional data is classified and protected, what uses of AIU technology are and are not acceptable, how security incidents are detected and managed, and how the University's growing use of artificial intelligence tools is governed.

**Scope**

This policy applies to all members of the AIU community, faculty, staff, administrators, students, contractors, vendors, and visitors, who use any information system, computing device, network, software platform, or data resource owned, leased, licensed, or managed by AIU, whether accessed on campus or remotely. It applies to all AIU-owned and AIU-managed systems, including the learning management system, student information system, financial systems, email and collaboration platforms, campus networks, classroom technology, and any cloud-based service procured or used institutionally. It applies to the use of personal devices that access AIU systems or store AIU data.

**Purpose**

The purposes of this policy are to:

- Establish the governance framework for information systems and technology decisions at AIU, with the CIO as the responsible institutional officer reporting to the President
- Define the data classification framework that governs how different categories of institutional data are handled, protected, and retained
- Establish the acceptable use standards for all members of the AIU community using institutional technology resources
- Define the information security standards, password management, access control, device management, antivirus, backup, and encryption, that protect AIU's systems and data

s

| | | | | |
|---|---|---|---|---|
| AIU AMERICAN INTERNATIONAL UNIVERSITY الجامعة الأمريكية الدولية | Policy Main Title | Information Systems and Technology Governance Policy | Effective Date | 14/06/2026 |
| | Category | Academic | Last Review date | |
| | Policy Number | ADM-004 | Next Review date | 14/06/2029 |
| | Responsible Entity | Chief Information Officer | Approved By | President |

- Establish the incident response framework for detecting, containing, and reporting security breaches and system failures
- Define the LMS governance framework that ensures Canvas is used consistently, reliably, and in support of learning outcome assessment
- Establish AIU's framework for the responsible institutional use of artificial intelligence tools
- Define the annual assessment and reporting cycle through which IT governance effectiveness is evaluated and used for improvement
- Demonstrate compliance with technology resources sufficient for educational objectives and data infrastructure supporting institutional effectiveness

**Definitions and Abbreviations**

**Chief Information Officer (CIO):** The senior institutional officer responsible for all information technology and systems governance at AIU, reporting directly to the President. The CIO leads the IT function, manages IT staff, and is the primary point of institutional accountability for technology infrastructure, information security, and data governance.

**Information System:** Any software application, database, network, computing device, or technology platform used by AIU to collect, store, process, transmit, or manage institutional data. Includes the LMS, SIS, email systems, financial systems, and institutional research platforms.

**Learning Management System (LMS):** AIU's designated online course management platform (Canvas) through which faculty deliver course content, administer assessments, and communicate with students. The LMS is the primary digital platform supporting teaching and student learning outcome assessment.

**Student Information System (SIS):** AIU's designated student records system (Banner) through which student enrolment, registration, grades, academic standing, and degree progress are managed. The SIS is the system of record for all student academic data.

**Institutional Data:** Any data collected, generated, processed, or maintained by AIU in the course of its educational, administrative, research, or operational activities, regardless of format or medium. Institutional data is AIU's property and is subject to this policy regardless of where it is stored.

**Data Steward:** A designated institutional role holder responsible for the accuracy, quality, appropriate use, and access governance of institutional data within their functional domain (e.g., the Registrar is data steward for student academic records; the HR Director for employee records).

**Information Security Incident:** Any event that results in or may result in unauthorised access to, disclosure of, alteration of, or destruction of institutional data or systems. Includes malware infections, phishing attacks, data breaches, system intrusions, and significant accidental data disclosures.

**Acceptable Use:** Use of AIU information systems and technology resources for purposes consistent with AIU's educational mission, institutional operations, applicable law, and this policy. Acceptable use standards are defined in Article 3.

**Authentication:** The process of verifying the identity of a user attempting to access an AIU system, typically through a combination of user identifier and password, or through multi-factor authentication.

**Multi-Factor Authentication (MFA)**: An authentication method requiring a user to provide two or more independent verification factors before being granted access, typically a password plus a one-time code sent to a registered device.

s

| | | | | |
|---|---|---|---|---|
| AIU AMERICAN INTERNATIONAL UNIVERSITY الجامعة الأمريكية الدولية | Policy Main Title | Information Systems and Technology Governance Policy | Effective Date | 14/06/2026 |
| | Category | Academic | Last Review date | |
| | Policy Number | ADM-004 | Next Review date | 14/06/2029 |
| | Responsible Entity | Chief Information Officer | Approved By | President |

**Backup:** A copy of institutional data maintained separately from the primary system to enable recovery in the event of data loss, system failure, or security incident.

**Policy**

**Article 1: Governing Principles**

The following principles govern AIU's information systems and technology governance:

a. Mission alignment: Technology decisions at AIU are made in service of the educational mission, not as independent institutional objectives. The LMS, the SIS, the institutional research infrastructure, and the security framework all exist to enable AIU to teach, assess, improve, and account for student learning.
b. Sufficiency: AIU's technology infrastructure is sufficient in scope, quality, currency, and kind to support its programs. Sufficiency is not assumed, it is assessed annually, with identified gaps addressed through the IT Strategic Plan and the annual budget cycle.
c. Security by design: Information security is a design principle, not an afterthought. Systems, processes, and user practices are designed to protect institutional data from the outset. The highest-risk data, student health records, financial information, authentication credentials, receives the most stringent protection.
d. Data stewardship: Institutional data is a shared asset with shared responsibility. The CIO is the institutional owner of the data governance framework; Data Stewards are responsible for data quality and access control within their functional domains; all users are responsible for handling the data they access in accordance with its classification.
e. Responsible innovation: AIU embraces technology and innovation as tools for improving educational outcomes and institutional effectiveness. Responsible innovation means adopting new technologies, including AI tools, with awareness of their risks, their ethical implications, and their impact on the academic integrity of the institution.
f. Accountability: Every use of AIU's technology systems is traceable. Authentication logs, access records, and system monitoring exist not to surveil users for its own sake but to enable investigation when something goes wrong and to provide evidence of institutional effectiveness to Accreditation agency.
g. Continuity: AIU maintains backup and disaster recovery capabilities sufficient to restore critical academic and administrative systems within defined timeframes. An institution that loses its student records, its assessment data, or its financial systems cannot demonstrate institutional effectiveness to any standard.

**Article 2: Information Technology Governance and the CIO**

The CIO reports directly to the President and is the institutional officer responsible for all information technology and systems governance. The CIO's authority and responsibilities are defined in GOV-004 (Presidential Authority and Delegation Policy) and are as follows:

s



a. Develop and maintain the IT Strategic Plan, aligned with the AIU RISE Strategy, and present it to the President annually for approval. The IT Strategic Plan addresses technology investment priorities, system lifecycle management, security posture, and service delivery standards for a three-year horizon.
b. Ensure that AIU's core academic and administrative systems, LMS, SIS, email, network infrastructure, and financial systems, are available, reliable, secure, and fit for purpose. System performance against the uptime and helpdesk KPIs in Article 11 is the primary measure of this responsibility.
c. Manage and develop the IT team, ensuring that staffing levels, skills, and professional development are adequate to support AIU's technology environment. The CIO reports on IT staffing capacity to the President annually.
d. Coordinate with the VPAA on academic technology requirements, including LMS standards, classroom technology, and the technology infrastructure supporting student learning outcome assessment. The CIO participates in academic planning discussions where technology investment decisions affect the assessment infrastructure required for accreditation.
e. Lead AIU's information security program, including annual security awareness training, security incident response, vulnerability management, and annual security posture review.
f. Oversee vendor and third-party technology relationships, ensuring that contracts include appropriate data protection clauses consistent with ADM-002 (Privacy and Personal Data Protection Policy).
g. Produce the Annual IT Governance Report, submitted to the President by 31 October each year and shared with the Board as part of the Annual Institutional Effectiveness Report.

The CIO documents all technology investment decisions and maintains a current technology asset register.

**Article 3: Acceptable Use**

All members of the AIU community who use institutional technology resources are bound by the following acceptable use standards.

| **Permitted Uses** | **Prohibited Uses** |
|---|---|
| **Teaching, learning, research, and scholarship activities** | Illegal activities under Kuwait law or applicable international law |
| **Academic administration and institutional operations** | Accessing, transmitting, or storing content prohibited under Kuwait law |

s



| | |
|---|---|
| **Professional development and communication related to AIU roles** | Harassment, bullying, or threatening communication |
| **Approved personal use that does not interfere with institutional systems or other users' access** | Bulk downloading of licensed database content in violation of license agreements |
| **Accessing licensed databases and electronic resources for educational and research purposes** | Installing unlicensed, unapproved, or pirated software on any AIU device or system |
| **Participating in AIU-sanctioned online learning and collaborative platforms** | Sharing, transferring, or disclosing authentication credentials to any other person |
| **Using approved AI tools in accordance with Article 8 of this policy and applicable academic integrity policies** | Attempting to circumvent security controls, access systems without authorization, or probe network vulnerabilities |
| **Reasonable incidental personal use during non-working hours where this does not compromise system performance or security** | Recreational use that materially impairs others' access to institutional computing resources |
| **Backing up institutional data to approved, authorized storage media or platforms** | Storing confidential or restricted institutional data on personal devices or unapproved cloud services |
| **Reporting suspected security incidents promptly to the CIO or IT helpdesk** | Concealing or failing to report a known or suspected security incident, data breach, or malware infection |

**Article 4: Data Classification**

All institutional data at AIU is classified into one of four categories. Data Stewards are responsible for classifying the data within their functional domains. Where data fits more than one category, it is handled according to the most sensitive applicable category:

s

| | | | | |
|---|---|---|---|---|
| AIU AMERICAN INTERNATIONAL UNIVERSITY الجامعة الأمريكية الدولية | Policy Main Title | Information Systems and Technology Governance Policy | Effective Date | 14/06/2026 |
| | Category | Academic | Last Review date | |
| | Policy Number | ADM-004 | Next Review date | 14/06/2029 |
| | Responsible Entity | Chief Information Officer | Approved By | President |

| Classification | Definition | Examples | Handling Requirements |
|---|---|---|---|
| **Public** | Information approved for unrestricted public disclosure that carries no confidentiality expectation | AIU website content; published academic catalogues; approved press releases; publicly posted policies | No special controls required; may be freely shared and published |
| **Internal** | Information intended for use within the AIU community that is not sensitive but is not intended for public distribution | Staff directories; internal announcements; general operational communications; non-sensitive committee minutes | Share within AIU; do not post publicly without authorization; basic access controls |
| **Confidential** | Sensitive information whose unauthorized disclosure could harm individuals, compromise institutional operations, or breach legal obligations | Student academic and financial records; employee personnel files; unpublished research; contract terms; financial forecasts; accreditation working documents | Restricted access on a need-to-know basis; encrypted in transit and at rest; not transmitted via personal email; subject to retention schedule |
| **Restricted** | The most sensitive category: personal, financial, or legal information whose unauthorized disclosure could cause serious harm, violate law, or result in significant institutional liability | Student health records; disability information; salary data; credit card and banking data; legal correspondence; authentication credentials; research participant data | Strictly controlled access; mandatory encryption; logged access; specific retention and disposal obligations; ADM-002 applies in full |

The CIO maintains a Data Classification Register documenting the classification of AIU's principal data holdings, the Data Steward responsible for each, and the applicable retention schedule. The Register is

s



reviewed annually and updated when new systems or data categories are introduced. Data Stewards are required to review and confirm the classification of data in their domain annually.

**Article 5: Information Security Standards**

**5.1 Authentication and Access Control**

The following authentication and access control standards apply to all AIU systems:

a. All users accessing AIU systems must authenticate with a unique, personal user identifier and a password meeting the minimum standards specified in this article. Shared accounts and shared passwords are prohibited, except in documented, CIO-approved operational circumstances where no individual account is technically possible.
b. Minimum password standards: The AIU requires at least 8 characters; complexity requiring at least three of the four character types (uppercase, lowercase, numeric, special character); must not include the user's name, student number, or AIU identifier; must not be a previously used password (system enforces a 10-password history).
c. All faculty and staff accounts with access to Confidential or Restricted data must use Multi-Factor Authentication (MFA). MFA is mandatory for all remote access to AIU systems regardless of data classification level. The CIO implements MFA on a phased rollout basis for all user categories.
d. Passwords must be changed at least every 180 days for standard users. Administrator and privileged accounts must be changed every 90 days. The system enforces these expiry cycles automatically. Where a user suspects their credentials have been compromised, they must change their password immediately and notify the IT helpdesk.
e. System sessions inactivity timeout: 15 minutes for systems holding Confidential or Restricted data; 30 minutes for standard systems. These values are enforced at the system level by the IT team.
f. Access to systems and data is granted on a least-privilege basis, users receive only the access permissions necessary for their specific role. Access rights are reviewed at least annually by the CIO and relevant Data Stewards, and immediately revoked or modified when a user's role changes or they separate from AIU.

**5.2 Device and Endpoint Security**

a. All AIU-owned computing devices must have approved antivirus and endpoint security software installed, active, and updated in real time. The CIO specifies the approved antivirus solution. Users must not disable, suspend, or circumvent antivirus software.
b. AIU-owned devices must not have unauthorized software installed. Software installations on institutional devices require IT helpdesk approval. The CIO maintains an approved software list. Software piracy is prohibited and constitutes a violation of this policy and applicable Kuwait law.
c. Where personal devices are used to access AIU systems or store AIU data (Bring Your Own Device), the device must meet minimum security standards specified by the CIO, including up-to-date operating system patches, approved antivirus software, and device encryption where Confidential or Restricted data is accessed. The CIO publishes and maintains BYOD minimum standards.

s



d. All AIU-owned laptops and mobile devices storing Confidential or Restricted data must use full-device encryption. Loss or theft of any AIU device must be reported to the IT helpdesk and the CIO within one hour of discovery.

**5.3 Network Security**

a. AIU's campus network is protected by firewalls, intrusion detection systems, and network monitoring maintained by the IT team. The CIO ensures that network security controls are reviewed at least annually and updated to reflect current threats.

b. All remote access to AIU internal systems requires the use of an authenticated VPN or equivalent secure access mechanism approved by the CIO. Direct remote access to internal systems without secure authentication is prohibited.

c. The AIU network provides separate network segments for: institutional systems (administrative and academic); student access; and guest access. Institutional systems are not accessible from the guest network.

d. Wireless network access requires AIU credential authentication. Open, unauthenticated wireless access to institutional systems is not permitted.

**5.4 Backup and Disaster Recovery**

a. All institutional data classified as Confidential or Restricted must be backed up at least daily to a secure backup system maintained separately from the primary system. The CIO maintains the backup schedule and backup infrastructure.

b. Backup integrity is verified monthly through documented recovery tests. Test results are reported to the President in the Annual IT Governance Report.

c. The CIO maintains a Disaster Recovery Plan (DRP) specifying the Recovery Time Objective (RTO) and Recovery Point Objective (RPO) for each critical AIU system. The DRP is reviewed and tested at least annually. Critical academic systems (LMS, SIS) must be recoverable within four hours.

d. The DRP addresses not only data recovery but also communication protocols for notifying students, faculty, and staff of system outages and recovery timelines.

**Article 6: Learning Management System (LMS) Governance**

The LMS (Canvas) is AIU's primary digital teaching and learning platform. Its governance is shared between the CIO (technical operation and availability) and the VPAA (academic use standards and faculty training). The following provisions apply:

a. All credit-bearing courses offered at AIU must have an LMS course shell, created by the IT team from the SIS enrolment data before the start of each semester. Faculty teaching the course are designated as the primary course instructor.

b. Faculty must publish their course syllabus, learning outcomes, assessment details, and primary course materials on Canvas at the start of each semester, consistent with the academic standards in ACA-001. The VPAA establishes the minimum Canvas course completion standards required for all AIU courses.

s



c. Student assessment submissions, grade records, and attendance data recorded in Canvas constitute part of the official course record. Faculty must not delete or modify submitted student work without documented academic justification approved by the relevant Dean.
d. LMS courses remain accessible to enrolled students for at least three years after the semester in which they were enrolled. Faculty may archive courses at the end of each semester; archived courses are retained for at least five years consistent with the retention schedule in ADM-002.
e. The CIO monitors LMS availability and resolves outages affecting course delivery as a Priority 1 incident. Where LMS unavailability affects scheduled assessments, the VPAA and Dean of Students coordinate academic contingency measures with faculty.
f. Third-party integrations with the LMS (plagiarism detection, proctoring, publisher content, AI tools) require CIO approval and must not compromise student data privacy. All LMS integrations are reviewed annually for security and compliance.

**Article 7: Incident Response**

An information security incident is any event that results in or may result in unauthorized access to, disclosure of, modification of, or destruction of institutional data or systems. The following response framework applies to all incidents:

a. Any member of the AIU community who discovers or suspects a security incident must report it immediately to the IT helpdesk and the CIO. Delayed reporting that increases the scope of an incident is itself a policy violation. The initial report may be verbal but must be followed by a written description within four hours.
b. The CIO classifies all reported incidents within two hours of notification and initiates the appropriate response level: Priority 1 (system-wide outage or Restricted data breach, immediate all-hands response); Priority 2 (significant data exposure or material system impairment, response within four hours); Priority 3 (isolated incident, limited impact, response within one working day).
c. For any incident involving actual or suspected unauthorized access to, or disclosure of, Confidential or Restricted data, the CIO notifies the President within two hours. The President determines whether affected data subjects must be notified, in coordination with the Privacy Officer per ADM-002.
d. The CIO maintains a Security Incident Register documenting every reported incident, its classification, the response taken, the resolution, and any corrective action implemented. The Register is reviewed quarterly and reported to the President annually.
e. Following every Priority 1 or Priority 2 incident, the CIO conducts a post-incident review within 10 working days, documenting root cause, effectiveness of the response, and corrective actions required. Post-incident reviews for incidents involving Restricted data are shared with the President and included in the Annual IT Governance Report.

s

| | | | | |
|---|---|---|---|---|
| AIU AMERICAN INTERNATIONAL UNIVERSITY الجامعة الأمريكية الدولية | Policy Main Title | Information Systems and Technology Governance Policy | Effective Date | 14/06/2026 |
| | Category | Academic | Last Review date | |
| | Policy Number | ADM-004 | Next Review date | 14/06/2029 |
| | Responsible Entity | Chief Information Officer | Approved By | President |

**Article 8: Artificial Intelligence - Institutional Use Framework**

Generative AI tools, applications that use large language models or related technologies to generate text, code, images, analysis, or other outputs, are increasingly used in higher education administration and instruction. AIU adopts a responsible innovation approach to AI: neither prohibiting AI tools across the board nor adopting them without governance. The following framework governs institutional AI tool use:

a. Academic use of AI tools by faculty and students is governed by the academic integrity provisions of STU-001 and ACA-005 (Library and Information Resources Policy) and by the course-level AI use policies published by faculty in their syllabi. This article governs administrative and operational AI tool use at the institutional level.
b. No AI tool that processes Confidential or Restricted institutional data may be used without prior written approval from the CIO and the Privacy Officer. This includes AI tools that process student records, personnel files, financial data, or any personally identifiable information. The CIO evaluates proposed AI tool uses against AIU's data privacy obligations under ADM-002.
c. Approved institutional AI tools are listed on the CIO's Approved Technology Register. Using an unapproved AI tool for institutional purposes -- particularly for processing Confidential or Restricted data, is a violation of this policy.
d. Faculty who use AI tools to assist in course design, assessment creation, or academic administration must do so in a manner consistent with academic integrity principles. AI-generated content used in official institutional communications, policy documents, or formal academic publications must be reviewed and approved by a qualified human professional before use.
e. The CIO monitors the AI tool landscape and reviews the Approved Technology Register at least annually, adding approved tools and removing those that no longer meet AIU's data protection standards or whose vendor practices have changed materially.
f. Outcomes of institutional AI tool use that affect students, including AI-assisted assessment tools, early alert systems, or student success analytics, must be disclosed to students in accordance with AIU's transparency obligations. Automated decisions about students must be reviewable by a qualified human officer.

**Article 9: Roles and Responsibilities**

| **Role** | **Information Systems and Technology Responsibilities** |
|---|---|
| **President** | Institutional accountability for information systems governance; approves this policy and material revisions; receives the Annual IT Governance Report; ensures adequate IT resources and staffing; endorses significant technology investments above the authority threshold of the CIO |

S



| | |
|---|---|
| **Chief Information Officer (CIO)** | Leads the Information Technology function; develops and maintains the IT Strategic Plan; oversees all institutional technology infrastructure, systems, and services; manages IT staff; ensures information security; administers data governance in coordination with the IR Director; produces the Annual IT Governance Report; serves as AIU's primary point of contact for data breaches and security incidents; reports directly to the President |
| **Vice President for Academic Affairs (VPAA)** | Coordinates with the CIO on academic technology needs including the LMS, academic databases, and classroom technology; represents academic requirements in IT investment decisions; ensures that IT planning supports the assessment and institutional effectiveness infrastructure required for accreditation |
| **IR Director** | Works with the CIO to maintain the data infrastructure supporting institutional research, assessment reporting, and accreditation evidence; administers the student information system in coordination with the Registrar; ensures data quality and accuracy for institutional effectiveness reporting |
| **Registrar** | Maintains the student information system as primary custodian of student academic records; coordinates with the CIO on system access controls and data integrity for academic records; ensures Banner or equivalent system is used correctly and in accordance with ADM-002 |
| **Data Stewards (Deans, HR Director, Finance Director, Registrar)** | Responsible for data quality and appropriate access controls within their functional domain; must approve requests for access to data in their domain; report data classification issues or breaches to the CIO; complete annual data governance training |
| **Faculty Members** | Use AIU IT systems in accordance with this policy and applicable academic policies; comply with LMS requirements and academic technology standards; report technology failures affecting teaching or assessment to |

s



| | |
|---|---|
| | the IT helpdesk; comply with AI use provisions in Article 8 and applicable academic integrity policies |
| **All Employees and Contractors** | Use AIU IT systems only for authorized purposes; comply with the Acceptable Use provisions of this policy; protect their authentication credentials; report suspected security incidents promptly; complete mandatory annual information security awareness training; return all institutional devices and data on separation from AIU |
| **Students** | Access AIU IT systems for academic and approved purposes; comply with the Student Acceptable Use provisions and the provisions of STU-001; protect their authentication credentials; report suspected security incidents to the IT helpdesk |

**Article 10: Security Awareness Training**

All AIU employees and contractors with access to institutional systems must complete mandatory annual information security awareness training. The following provisions apply:

a. The CIO designs or procures the annual security awareness training program and delivers it at the start of each academic year, with all employees completing training before the fifth week of the academic year. The program covers: this policy's key provisions; data classification and handling; phishing and social engineering recognition; password hygiene; incident reporting; and AI tool governance.
b. New employees complete security awareness training as part of institutional onboarding, before being granted access to systems holding Confidential or Restricted data.
c. Completion of security awareness training is tracked by IT and HR. Employees who have not completed training by the published deadline may have their access to systems holding Confidential or Restricted data temporarily suspended pending completion.
d. The CIO provides targeted additional training for: Data Stewards (on data classification and access governance); IT staff (on advanced security practices); and any employee group identified as high-risk through phishing simulation exercises or security incident patterns.
e. The effectiveness of the security awareness training program is evaluated annually through: security incident rates; phishing simulation test results (where used); and inclusion of training effectiveness in the Annual IT Governance Report.

**Article 11: Assessment and Annual Reporting**

The CIO assesses IT governance effectiveness annually using the following Key Performance Indicators:

s



| KPI | Measurement | Target |
|---|---|---|
| **System availability (core academic systems: LMS, SIS, email)** | IT monitoring logs: percentage uptime of core academic systems during published operating hours | >=99.5% uptime per academic year |
| **IT helpdesk resolution time** | Helpdesk ticket records: percentage of Priority 1 (critical) tickets resolved within 4 hours; Priority 2 within 24 hours; Priority 3 within 5 working days | P1: >=90% within 4 hours; P2: >=90% within 24 hours; P3: >=95% within 5 days |
| **Security incident rate** | Number of confirmed security incidents per academic year | Trend reduction year-on-year; zero incidents involving Restricted data |
| **Security awareness training completion** | HR/IT records: percentage of employees completing annual security awareness training | >=95% of all employees annually |
| **Data classification compliance** | Annual audit: percentage of institutional data holdings correctly classified and protected | >=90% compliance in annual audit |
| **User satisfaction with IT services** | Annual IT User Satisfaction Survey: percentage of faculty and staff rating overall IT services as Satisfactory or above | >=80% satisfaction |
| **Backup and recovery reliability** | Monthly backup verification tests: percentage of successful recovery tests | 100% monthly verification; recovery within 4 hours for critical systems |

s



| | | |
|---|---|---|
| **Password and access control compliance** | Quarterly IT audit: accounts with expired passwords, dormant accounts, and privileged access reviews | Zero unresolved critical access control findings after 30-day remediation period |

The CIO prepares the Annual IT Governance Report by 31 October each year, covering the preceding academic year. The Report is submitted to the President and shared with the Board as part of the Annual Institutional Effectiveness Report (IE-002). The Annual IT Governance Report includes: KPI performance against all targets; security incident summary (de-identified); data classification audit results; system availability data for all core systems; backup and recovery verification results; security training completion rates; the CIO's assessment of AIU's current technology posture relative to Accreditation agency requirements; and proposed priorities for the following year.

The Annual IT Governance Report also serves as evidence for Accreditation agency that AIU's technology infrastructure is actively managed, assessed, and improved. Accreditation agency visiting teams regularly request IT system availability data, incident records, and evidence of security governance as part of Standard 3 review. The Annual IT Governance Report is the primary institutional document responding to these requests.

**Procedures**

**Information Security Incident Reporting and Response**

1. Any user who discovers or suspects a security incident contacts the IT helpdesk by phone (for urgent/Priority 1 matters) or email (for non-urgent matters) immediately upon discovery. The report includes: a description of what was observed; the system(s) affected; the data potentially involved; the time of discovery; and the user's contact details.
2. The IT helpdesk logs the report and notifies the CIO within 30 minutes of receipt. The CIO classifies the incident within two hours of the initial report. For Priority 1 incidents, the CIO notifies the President immediately. For Priority 2 incidents, the CIO notifies the President within four hours.
3. The CIO initiates the response appropriate to the incident classification, coordinating with IT staff, Data Stewards, and external vendors as required. The CIO documents all response actions in the Security Incident Register in real time.
4. Where the incident involves Confidential or Restricted data, the CIO notifies the Privacy Officer (per ADM-002) within two hours, who assesses whether affected individuals must be notified. The Privacy Officer determines the notification approach in consultation with the President and Legal Counsel.
5. The CIO resolves the incident, documents the resolution, and initiates a post-incident review for Priority 1 and 2 incidents within 10 working days. The post-incident review report is filed with the Security Incident Register and included in the Annual IT Governance Report.

s

| | | | | |
|---|---|---|---|---|
| AIU AMERICAN INTERNATIONAL UNIVERSITY الجامعة الأمريكية الدولية | Policy Main Title | Information Systems and Technology Governance Policy | Effective Date | 14/06/2026 |
| | Category | Academic | Last Review date | |
| | Policy Number | ADM-004 | Next Review date | 14/06/2029 |
| | Responsible Entity | Chief Information Officer | Approved By | President |

**Technology Procurement and Approval**

1. Any department head or academic officer wishing to procure a new technology system, software platform, or AI tool submits a Technology Procurement Request to the CIO. The Request describes: the proposed system/tool; its purpose and intended users; the data it will process (and its classification); the vendor; the proposed cost; and the business or educational justification.
2. The CIO reviews the Request within five working days for: technical compatibility with existing systems; data security and privacy implications (in consultation with the Privacy Officer where Confidential or Restricted data is involved); licensing and contractual terms; and alignment with the IT Strategic Plan. Where an AI tool is proposed, the CIO applies the Article 8 AI governance framework.
3. The CIO approves, conditionally approves, or declines the Request and communicates the decision in writing within 10 working days. Approved technology is added to the Approved Technology Register. Procurement then proceeds through the standard procurement process (FIN-005).
4. For technology investments above KD 25,000, the CIO recommendation is submitted to the President for approval before procurement proceeds. For investments above KD 100,000, the process follows the Board authority requirements in FIN-002.

**Annual IT Governance Review**

1. By 1 September each year, the CIO initiates the annual IT governance review, compiling: KPI data for the preceding year; the Security Incident Register; backup verification records; security training completion data; and system availability logs.
2. The CIO conducts a technology posture assessment, evaluating AIU's current systems and security controls against: current Accreditation agency expectations; Kuwait cybercrime law (Law No. 2 of 2001) compliance; the previous year's Annual IT Governance Report recommendations; and emerging technology risks identified through professional monitoring.
3. The CIO prepares the Annual IT Governance Report and the updated IT Strategic Plan priorities by 31 October, submitting them to the President. The President reviews and endorses the Report before it is incorporated in the Annual Institutional Effectiveness Report.
4. The CIO presents a summary of the Annual IT Governance Report to the Board Academic Affairs Committee at its December meeting, enabling the Board to satisfy its Accreditation agency oversight obligations. Material security risks or technology investment needs above the presidential authority threshold are escalated to the Board Finance Committee.

| | |
|---|---|
| **President Signature** | Signature: _____ Date: _____ |