

 AMERICAN INTERNATIONAL UNIVERSITY الجامعة الأمريكية الدولية	Policy Main Title	Privacy and Personal Data Protection Policy	Effective Date	14/06/2026
	Category	Administration and Campus Operations	Last Review date	
	Policy Number	ADM-002	Next Review date	14/06/2029
	Responsible Entity	VP Administration	Approved By	President

Overview

Personal data, the information AIU holds about students, employees, applicants, research participants, contractors, and visitors, is one of the most consequential categories of institutional asset. It is consequential because its misuse, loss, or unauthorized disclosure harms real people: students whose academic records or immigration status are exposed, employees whose payroll or health data is leaked, research participants whose identities are revealed despite assurances of confidentiality. Accrediting agency requires that institutions demonstrate honest, ethical, and sound business practices. There is no domain in which that requirement is more concretely tested than in how an institution handles the personal data of the people who trust it.

This policy establishes AIU's a framework for the collection, use, storage, protection, disclosure, and disposal of all personal data held by or on behalf of AIU. It is grounded in AIU's Kuwait legal context and to the privacy standards expected of accredited institutions. AIU applies a principles-based privacy framework anchored in: applicable Kuwait laws (Kuwait Law No. 2 of 2001 on Cybercrime; Kuwait Labor Law No. 6 of 2010); PUC student data requirements; and the internationally recognized privacy principles of purpose limitation, data minimization, accuracy, storage limitation, integrity and confidentiality, and accountability. AIU is committed to compliance with any comprehensive Kuwait data protection legislation when enacted.

Scope

This policy applies to all personal data collected, generated, processed, stored, transmitted, shared, or disposed of by AIU or on AIU's behalf, regardless of the format (digital, paper, audio, video), the system in which it is held, or the unit responsible for it. It applies to all AIU employees, faculty, staff, contractors, third-party service providers operating on AIU systems, and students in their capacity as data handlers in research or other supervised activities. It covers all categories of personal data, student data, employee data, research participant data, vendor data, and operational data collected through AIU's systems, devices, and facilities.

Purpose

The purposes of this policy are to:

- Establish AIU's commitment to collecting, using, and protecting personal data in a manner that respects the dignity, privacy, and rights of every individual whose data it holds
- Define the lawful bases on which personal data is collected and processed, ensuring that every data collection activity can be justified by a legitimate institutional purpose
- Specify the data subject rights, access, correction, erasure, portability, objection, and complaint, that AIU recognizes and the process through which those rights may be exercised
- Define the data categories held by AIU, the retention period applicable to each, and the secure disposal methods required when the retention period expires
- Establish the data security standards and incident response framework that protect personal data from unauthorized access, loss, or disclosure

 AMERICAN INTERNATIONAL UNIVERSITY الجامعة الأمريكية الدولية	Policy Main Title	Privacy and Personal Data Protection Policy	Effective Date	14/06/2026
	Category	Administration and Campus Operations	Last Review date	
	Policy Number	ADM-002	Next Review date	14/06/2029
	Responsible Entity	VP Administration	Approved By	President

- Define the roles and responsibilities of every person in the AIU community who handles personal data, from the President to individual employees
- Establish the privacy governance structure, Privacy Officer, Data Processing Register, Privacy Notice, training requirements, that makes privacy compliance auditable and sustainable
- Demonstrate compliance with honest, ethical, and sound institutional operations, institutional integrity, and ongoing institutional effectiveness

Definitions and abbreviations

Personal Data: Any information that identifies or can reasonably be used to identify a living natural person directly (such as name, civil ID number, or photograph) or indirectly when combined with other available information. The definition applies regardless of the medium in which the data is held.

Sensitive Personal Data: A sub-category of personal data warranting heightened protection because of the particular harm its disclosure could cause: health and medical data; biometric data used for identification; financial data beyond general salary ranges; data about religious beliefs, political opinions, or ethnic origin; criminal history; and immigration status.

Processing: Any operation or set of operations performed on personal data, including collection, recording, organization, structuring, storage, adaptation, retrieval, consultation, use, disclosure, dissemination, alignment, combination, restriction, erasure, or destruction.

Data Subject: The natural person to whom personal data relates. At AIU, data subjects include: current, former, and prospective students; current, former, and prospective employees; research participants; and any other individual whose personal data AIU holds.

Lawful Basis: The legally recognized ground that justifies processing personal data. Recognized lawful bases at AIU include: the performance of an educational or employment contract; compliance with a legal obligation; protection of vital interests; legitimate institutional interest; and the data subject's freely given, specific, and informed consent.

Privacy Officer: The institutional officer designated to oversee AIU's privacy program, respond to data subject requests and complaints, investigate data incidents, maintain the Data Processing Register, and serve as the primary institutional contact for privacy matters.

Data Processing Register: The institutional record maintained by the Privacy Officer documenting all categories of personal data held by AIU, the purpose and lawful basis of processing, data stewardship responsibilities, retention periods, and applicable security measures.

Privacy Notice: A clear, concise, and accessible statement provided to data subjects at the point of data collection, describing what data is collected, why it is collected, how it will be used, who it may be shared with, how long it will be retained, and the data subject's rights.

Data Incident: Any event resulting in, or with the potential to result in, the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data. Includes both confirmed breaches and near misses.

Data Minimization: The principle that only the personal data that is necessary for the specified, legitimate purpose is collected, and that data is not collected in anticipation of possible future uses not yet identified.

Purpose Limitation: The principle that personal data collected for a specific, legitimate purpose is not used for any other purpose incompatible with the original purpose without the data subject's consent or a valid legal basis.

 AMERICAN INTERNATIONAL UNIVERSITY الجامعة الأمريكية الدولية	Policy Main Title	Privacy and Personal Data Protection Policy	Effective Date	14/06/2026
	Category	Administration and Campus Operations	Last Review date	
	Policy Number	ADM-002	Next Review date	14/06/2029
	Responsible Entity	VP Administration	Approved By	President

Storgae Limitation: The principle that personal data is kept in a form that identifies data subjects only for as long as is necessary for the specified purpose, after which it is anonymized, disposed of securely, or transferred to permanent archival storage as specified in this policy.

Data Steward: An institutional role holder (typically a director or head of department) designated as responsible for the accuracy, integrity, appropriate use, and security of personal data within a specific domain.

Consent: A freely given, specific, informed, and unambiguous indication of a data subject's agreement to the processing of their personal data. Consent must be an active affirmation, silence, inaction, or pre-ticked boxes do not constitute consent.

Policy

Article 1: Governing Principles of Privacy and Data Protection

AIU's approach to personal data is governed by the following principles, derived from internationally recognized data protection standards and adapted to the Kuwait context:

- Lawfulness, fairness, and transparency:** Personal data is collected and processed on a valid lawful basis, in a manner that is fair to the data subject, and with clear communication about what data is collected and why. Surprise collection, collecting data for purposes not disclosed to the data subject, is not acceptable.
- Purpose limitation:** Personal data is collected for a specific, explicit, and legitimate purpose and not processed in a manner incompatible with that purpose. Survey data collected for institutional improvement is not repurposed to identify individual critics. Research participant data is not used for administrative purposes without explicit separate consent.
- Data minimization:** Only the personal data that is strictly necessary for the stated purpose is collected. AIU does not collect data speculatively, in bulk, or in anticipation of uses not yet identified. Admission forms collect what is needed for admission decisions, not lifetime behavioral profiles.
- Accuracy:** Personal data is kept accurate and, where necessary, up to date. Data subjects are encouraged to notify AIU of changes. AIU maintains processes to correct inaccurate data promptly.
- Storage limitation:** Personal data is held only for as long as is necessary for the purpose for which it was collected, or as required by applicable law. The retention schedule in Article 9 defines the maximum retention period for each data category. Data is securely disposed of at the end of the applicable retention period.
- Integrity and confidentiality:** Personal data is protected against unauthorized or unlawful access, accidental loss, destruction, or damage, using appropriate technical and organizational security measures. The standard of protection is proportionate to the sensitivity of the data and the harm that could result from a breach.
- Accountability:** AIU does not merely assert these principles; it can demonstrate compliance. The Data Processing Register, Privacy Notice, training records, incident log, and data subject request log constitute the evidence base for AIU's privacy accountability.

 AMERICAN INTERNATIONAL UNIVERSITY الجامعة الأمريكية الدولية	Policy Main Title	Privacy and Personal Data Protection Policy	Effective Date	14/06/2026
	Category	Administration and Campus Operations	Last Review date	
	Policy Number	ADM-002	Next Review date	14/06/2029
	Responsible Entity	VP Administration	Approved By	President

Article 2: Data Categories and Lawful Bases

The following categories of personal data are held by AIU. For each category, the lawful basis for processing is identified. Processing that cannot be justified against a lawful basis in this table is not authorized. The complete Data Processing Register, maintained by the Privacy Officer, provides detailed specifications for each data category:

Data Category	Examples	Lawful Basis	Retention
Student Data			
Enrolment and academic records	Name, civil ID, grades, transcript, degree certificate, academic standing, program enrolled, GPA	Performance of an educational contract; legal obligation (PUC); accreditation	Academic records: permanent. Registration data: 10 years after graduation
Student health and disability data	Medical certificates, accommodation requests, disability documentation	Vital interests; legal obligation; consent	Duration of enrolment plus 7 years
Financial and scholarship data	Tuition payments, scholarship awards, financial holds, sponsor details	Performance of contract; legal obligation	10 years after last financial transaction
Student conduct and disciplinary records	Misconduct allegations, investigation records, sanctions imposed	Legitimate institutional interest; legal obligation	7 years after graduation or last enrolment
Employee and Applicant Data			
HR and employment records	Name, civil ID, passport, employment contract,	Performance of contract; legal	Duration of employment plus 10 years

 AMERICAN INTERNATIONAL UNIVERSITY الجامعة الأمريكية الدولية	Policy Main Title	Privacy and Personal Data Protection Policy	Effective Date	14/06/2026
	Category	Administration and Campus Operations	Last Review date	
	Policy Number	ADM-002	Next Review date	14/06/2029
	Responsible Entity	VP Administration	Approved By	President

	salary, performance reviews, leave records	obligation (Kuwait Labor Law)	
Recruitment data (unsuccessful applicants)	Application, CV, interview notes, reference checks	Pre-contractual steps; consent	1 year after rejection, then securely destroyed
Payroll and financial data	Bank details, salary, deductions, end-of-service gratuity	Performance of contract; legal obligation	10 years minimum
Operational and Third-Party Data			
Vendor and contractor contact data	Names, email, phone, civil ID of authorized signatories	Legitimate interest; performance of contract	Duration of relationship plus 7 years
Research participant data	Consent forms, survey responses, interview data, personal identifiers	Consent; research ethics approval	As specified in research protocol; minimum 5 years
CCTV and access control data	Video footage, door access logs from security systems	Legitimate interest campus safety	Maximum 30 days unless retained for an active investigation
Online learning and LMS data	Login records, course access, assignment submissions, video attendance	Performance of educational contract; legitimate interest	Duration of enrolment plus 5 years

Article 3: Privacy Notice and Consent

3.1 Privacy Notice Obligations

AIU provides a Privacy Notice to data subjects at or before the point of personal data collection in all circumstances. The Privacy Notice is not a legal waiver, it is a genuine communication designed to inform

 AMERICAN INTERNATIONAL UNIVERSITY الجامعة الأمريكية الدولية	Policy Main Title	Privacy and Personal Data Protection Policy	Effective Date	14/06/2026
	Category	Administration and Campus Operations	Last Review date	
	Policy Number	ADM-002	Next Review date	14/06/2029
	Responsible Entity	VP Administration	Approved By	President

the data subject about what data is collected, why, and what their rights are. A Privacy Notice that is designed to be unread is not a compliant Privacy Notice.

Every AIU Privacy Notice must state:

- The identity and contact details of AIU as the data controller, and the contact details of the Privacy Officer
- The specific categories of personal data being collected
- The purpose(s) for which the data is collected and the lawful basis for each purpose
- Whether any data will be shared with third parties, and if so, with whom and on what basis
- The retention period applicable to the data or the criteria used to determine it
- The data subject's rights under this policy and how to exercise them
- Whether providing the data is a statutory or contractual requirement, or voluntary, and the consequences of not providing it

3.2 Consent as a Lawful Basis

Where AIU relies on consent as the lawful basis for processing, the consent must be freely given, specific, informed, and unambiguous. The following conditions apply:

- Consent is obtained through a clear, positive action by the data subject — a signed consent form, a ticked checkbox, or a verbal confirmation recorded in writing. Pre-ticked boxes, implied consent from inaction, or consent bundled into lengthy terms and conditions without prominence do not meet this standard.
- Consent is granular where multiple processing purposes exist — the data subject can consent to one purpose and not another. Bundled blanket consent for all possible future uses is not valid.
- A data subject who declines to provide consent for a purpose that is not a contractual or legal requirement is not penalized. Where consent is required for a service that AIU could not provide without it, this dependency is clearly communicated in advance.
- Consent may be withdrawn at any time. The withdrawal is as easy as the giving of consent. Withdrawal does not affect the lawfulness of processing carried out before the withdrawal.

3.3 Survey and Research Data

Personal data collected through surveys, including student course evaluations, satisfaction surveys, graduate surveys, and employer surveys, is subject to specific provisions:

- Survey results are reported in aggregate form. Individual responses identifying specific data subjects are not disclosed to faculty, supervisors, or any person with a direct evaluative relationship with the respondent, except where the law requires.
- Student course and program evaluations are not disclosed to the relevant faculty member or instructor until after final grades for the relevant course have been submitted and confirmed.
- Verbatim comments from surveys may be reproduced in internal reports or external publications only in anonymized form that prevents identification of the individual respondent.

 AMERICAN INTERNATIONAL UNIVERSITY الجامعة الأمريكية الدولية	Policy Main Title	Privacy and Personal Data Protection Policy	Effective Date	14/06/2026
	Category	Administration and Campus Operations	Last Review date	
	Policy Number	ADM-002	Next Review date	14/06/2029
	Responsible Entity	VP Administration	Approved By	President

- d. Research involving human participants requires research ethics approval from AIU's designated ethics review process before any data is collected. The approved research protocol governs all data collection, use, retention, and disposal for that project.

Article 4: Data Subject Rights

AIU recognizes the following rights of data subjects and maintains a process for exercising them. Data subject requests are submitted to the Privacy Officer and are responded to within the timeframes specified. The right to exercise these rights does not depend on Kuwait having enacted a comprehensive data protection law, AIU commits to respecting these rights as a matter of institutional integrity and international good practice:

Right	What It Means for AIU	How to Exercise
Right to access	The data subject may request confirmation of whether AIU holds personal data about them and a copy of that data in an accessible format	Submit a Data Subject Request to the Privacy Officer; response within 30 calendar days
Right to correction	The data subject may request correction of inaccurate or incomplete personal data	Submit a correction request to the Privacy Officer or the relevant data steward; corrected within 15 working days
Right to erasure (where applicable)	The data subject may request deletion of personal data where it is no longer necessary for the purpose collected, where consent is withdrawn, or where processing is unlawful - subject to legal retention obligations	Submit an erasure request to the Privacy Officer; AIU advises within 30 days whether the request can be fulfilled or is subject to a retention obligation
Right to restriction of processing	The data subject may request that AIU restrict processing of their data while a correction or objection is pending	Submit a restriction request to the Privacy Officer; restriction applied within 5 working days of confirmation

 AMERICAN INTERNATIONAL UNIVERSITY الجامعة الأمريكية الدولية	Policy Main Title	Privacy and Personal Data Protection Policy	Effective Date	14/06/2026
	Category	Administration and Campus Operations	Last Review date	
	Policy Number	ADM-002	Next Review date	14/06/2029
	Responsible Entity	VP Administration	Approved By	President

Right to data portability	The data subject may request their personal data in a structured, machine-readable electronic format	Submit a portability request to the Privacy Officer; data provided within 30 calendar days
Right to object	The data subject may object to processing based on legitimate interest, including direct marketing	Submit an objection to the Privacy Officer; processing suspended pending review unless AIU has compelling legitimate grounds
Right to withdraw consent	Where processing is based on consent, the data subject may withdraw consent at any time without penalty	Withdraw consent through the mechanism specified in the relevant consent notice or by contacting the Privacy Officer
Right to complain	The data subject may lodge a complaint with AIU's Privacy Officer or with the relevant Kuwait regulatory authority	Address complaints to the Privacy Officer; escalation to Kuwait regulatory authority available where AIU's response is unsatisfactory

All data subject requests are logged by the Privacy Officer in the Data Subject Request Register, including the date received, the nature of the request, the response provided, and the date of response. Where a request is declined, the grounds for refusal are documented and communicated to the data subject in writing. The data subject has the right to escalate a refused request to the VP Administration and, where that does not resolve the matter, to the relevant Kuwait regulatory authority.

Article 5: Data Sharing and Third-Party Disclosure

AIU does not sell personal data. Personal data is shared with third parties only where a valid lawful basis and a documented disclosure agreement exist. The following categories of third-party disclosure are authorized:

 AMERICAN INTERNATIONAL UNIVERSITY الجامعة الأمريكية الدولية	Policy Main Title	Privacy and Personal Data Protection Policy	Effective Date	14/06/2026
	Category	Administration and Campus Operations	Last Review date	
	Policy Number	ADM-002	Next Review date	14/06/2029
	Responsible Entity	VP Administration	Approved By	President

- a. Kuwait government authorities: AIU may share personal data with the Private Universities Council, the Ministry of Education, the Ministry of Higher Education, and other Kuwait government bodies where required by law or PUC regulation. Disclosure is limited to the data elements required to fulfil the specific obligation.
- b. Accrediting agency and accreditation bodies: AIU may share institutional data, including aggregate student data and, where required, faculty personnel data, with Accrediting agency and Program accreditation bodies (AACSB, ABET, and others) as part of accreditation review processes. Identifiable student data shared with Accrediting agency is limited to what the accreditation process specifically requires.
- c. Affiliate and partner universities: AIU's Program partnerships with Wayne State University and the University of Miami require the sharing of specific student and academic data for purposes of Program delivery, student exchange, and transcript recognition. Data sharing with partner universities is governed by data sharing agreements specifying the data elements shared, the purposes of sharing, the security obligations of the receiving party, and the prohibition on further disclosure.
- d. Technology and service providers: AIU shares personal data with third-party providers of essential services, the LMS provider, student information system provider, payroll processor, and others, only to the extent necessary for service delivery. All such providers are bound by written data processing agreements that require them to process data only on AIU's documented instructions, maintain adequate security, not sub-process without AIU's authorization, and return or destroy data at the end of the service relationship.
- e. Emergency disclosures: AIU may disclose personal data to emergency services or security authorities without prior consent where disclosure is necessary to protect the vital interests of the data subject or another person, for example, in a medical emergency, a credible threat to safety, or an active criminal investigation.
- f. All third-party disclosures not listed above require Privacy Officer approval and VP Administration endorsement before any data is shared.

Article 6: Data Security

Personal data held by AIU is protected by security measures proportionate to the sensitivity of the data and the risk posed by its potential compromise. The IT Department is responsible for implementing and maintaining the technical security measures. The following minimum standards apply:

- a. Access control: Access to personal data is restricted to employees with a documented, role-specific need. Access rights are reviewed at least annually and immediately updated when an employee's role changes or they leave AIU. No system administrator holds unrestricted, unmonitored access to all personal data.
- b. Encryption: Personal data stored on portable devices (laptops, USB drives, mobile phones) and transmitted over public or external networks is encrypted. Unencrypted personal data is not transmitted by email unless the recipient is an authorized party and the data is not sensitive.

 AMERICAN INTERNATIONAL UNIVERSITY الجامعة الأمريكية الدولية	Policy Main Title	Privacy and Personal Data Protection Policy	Effective Date	14/06/2026
	Category	Administration and Campus Operations	Last Review date	
	Policy Number	ADM-002	Next Review date	14/06/2029
	Responsible Entity	VP Administration	Approved By	President

- c. Network security: AIU maintains firewalls, intrusion detection systems, and network monitoring appropriate to the data it holds. The IT Department conducts penetration testing at least annually and addresses identified vulnerabilities within risk-based timelines.
- d. Secure disposal: At the end of the applicable retention period, personal data is disposed of securely. Paper records containing personal data are shredded by a cross-cut shredder or destroyed by an authorized confidential waste contractor. Digital data is deleted using a method that prevents recovery, including degaussing or secure overwrite for magnetic storage, and physical destruction for solid-state storage where required.
- e. Physical security: Paper records containing personal data are stored in locked cabinets accessible only to authorized personnel. Campus areas housing sensitive data systems are access-controlled. CCTV systems are secured against unauthorized access and footage is not accessible from outside the security control infrastructure.
- f. Third-party security: Service providers with access to AIU's personal data are required to demonstrate security standards at least equivalent to AIU's own through contractual warranties, ISO 27001 certification, or equivalent evidence. The IT Director reviews third-party security assessments annually.

Article 7: CCTV and Surveillance

AIU operates CCTV and access control systems on campus for the purpose of maintaining the safety and security of students, staff, and campus assets. The following provisions govern surveillance data:

- a. CCTV cameras are positioned and operated for security and safety purposes only. Cameras are not used to monitor employee or student academic performance, manage working conditions beyond what is strictly necessary for safety, or conduct covert surveillance of any person.
- b. Signage notifying of CCTV operation is posted at all entrances to areas covered by cameras. The notification identifies AIU as the operator and provides contact details for privacy enquiries.
- c. Routine CCTV footage is retained for a maximum of 30 calendar days, after which it is automatically overwritten. Footage relevant to an ongoing security investigation is retained until the investigation and any appeal are concluded.
- d. CCTV footage is accessed only by the Security Officer, the VP Administration, and where required by law, by police or judicial authorities. Requests for footage from any other party, including faculty or general staff, are routed through the Privacy Officer.
- e. Video and audio recordings made through educational technology, lecture recordings, video conferencing sessions, online tutorials, are used only for the educational purposes stated at the time of recording. Recordings are not shared beyond enrolled students and authorized faculty without consent, except where required by law.

Article 8: Data Incident Management

A data incident, any event resulting in, or with the potential to result in, unauthorized access, disclosure, loss, or alteration of personal data, must be reported, investigated, and managed promptly. The severity of the response is calibrated to the severity of the incident:

 AMERICAN INTERNATIONAL UNIVERSITY الجامعة الأمريكية الدولية	Policy Main Title	Privacy and Personal Data Protection Policy	Effective Date	14/06/2026
	Category	Administration and Campus Operations	Last Review date	
	Policy Number	ADM-002	Next Review date	14/06/2029
	Responsible Entity	VP Administration	Approved By	President

Severity	Examples	Required Response
Low	Accidental disclosure to a wrong internal recipient where data is retrieved and not further shared; minor system misconfiguration with no evidence of access	Privacy Officer notified within 1 working day; incident documented; corrective action within 10 working days; no regulatory notification required
Moderate	Loss of an unencrypted device containing personal data; disclosure to an external party not authorized to receive the data; phishing attack resulting in credential compromise	Privacy Officer notified immediately; VP Administration informed within 4 hours; affected data subjects notified within 72 hours where required; regulatory authority notification assessed; formal investigation within 5 working days
High	Ransomware affecting systems containing personal data; large-scale data breach affecting multiple data subjects; disclosure of sensitive categories of personal data	VP Administration and President notified immediately; Privacy Officer leads incident response team; regulatory authority notified within 72 hours; Board notified at next meeting or earlier if warranted; external counsel and IT forensics engaged as needed
Research-specific	Unauthorized disclosure of research participant identifiable data	Research Ethics Committee and Privacy Officer notified immediately; follow research participant data breach protocol; regulatory notification assessed

Every data incident, regardless of severity, is recorded in the Data Incident Register maintained by the Privacy Officer. The register records: the date and nature of the incident; the data affected (categories and approximate number of individuals); the cause; the immediate response; the corrective actions taken; and the date of closure. The Register is reviewed quarterly by the VP Administration and annually by the Board Audit and Risk Committee as part of AIU's risk oversight. A pattern of low-severity incidents may indicate a systemic control failure warranting a more comprehensive review.

 AMERICAN INTERNATIONAL UNIVERSITY الجامعة الأمريكية الدولية	Policy Main Title	Privacy and Personal Data Protection Policy	Effective Date	14/06/2026
	Category	Administration and Campus Operations	Last Review date	
	Policy Number	ADM-002	Next Review date	14/06/2029
	Responsible Entity	VP Administration	Approved By	President

Article 9: Data Retention and Secure Disposal

Personal data is retained only for as long as is necessary for the purpose for which it was collected, or as required by applicable Kuwait law or accreditation requirements. The following retention schedule applies. At the end of the applicable period, data is disposed of through the secure disposal method defined in Article 6:

Record Category	Retention Period	Basis
Student academic records and transcripts	Permanent — never destroyed	Accreditation, legal obligation, graduate verification requests
Student enrolment and registration records	10 years after graduation or last enrolment	PUC requirements; legal obligation
Student disciplinary records	7 years after graduation or last enrolment	Institutional policy; legal obligation
Student health and accommodation records	Duration of enrolment plus 7 years	Legal obligation; potential claims
Employee personnel files (active)	Duration of employment plus 10 years	Kuwait Labour Law; legal obligation
Employee payroll records	10 years minimum after last payment	Kuwait Labour Law; tax and audit requirements
Unsuccessful recruitment records	1 year after rejection decision, then destroyed	Legitimate interest; potential discrimination claims
CCTV footage - routine	30 calendar days, then overwritten	Security purpose; proportionality

 AMERICAN INTERNATIONAL UNIVERSITY الجامعة الأمريكية الدولية	Policy Main Title	Privacy and Personal Data Protection Policy	Effective Date	14/06/2026
	Category	Administration and Campus Operations	Last Review date	
	Policy Number	ADM-002	Next Review date	14/06/2029
	Responsible Entity	VP Administration	Approved By	President

CCTV footage - retained for active investigation	Until investigation is concluded and any appeal resolved	Legal obligation; legitimate interest
Research data containing personal data	As specified in approved research protocol; minimum 5 years after publication	Research integrity standards; ethics requirements
Vendor and contractor contact records	Duration of relationship plus 7 years	Legal obligation; contract enforcement
Financial records	10 years from the relevant financial year	Kuwait law; audit requirements
Survey and assessment responses	Anonymised aggregate retained indefinitely; identifiable data destroyed after analysis	Purpose limitation; proportionality
Privacy incident records	10 years from incident closure	Legal obligation; accountability

The Privacy Officer, in coordination with the IT Department, the Registrar, and the HR Director, maintains a Data Retention Schedule that maps every category of personal data in the Data Processing Register to its applicable retention period and disposal method. The Retention Schedule is reviewed annually and updated where changes in law, accreditation requirements, or institutional activities affect retention obligations.

Article 10: Roles and Responsibilities

Privacy at AIU is a shared institutional responsibility. Every member of the AIU community who handles personal data has a defined role in protecting it:

 AMERICAN INTERNATIONAL UNIVERSITY الجامعة الأمريكية الدولية	Policy Main Title	Privacy and Personal Data Protection Policy	Effective Date	14/06/2026
	Category	Administration and Campus Operations	Last Review date	
	Policy Number	ADM-002	Next Review date	14/06/2029
	Responsible Entity	VP Administration	Approved By	President

Role	Privacy Responsibilities
President	Holds ultimate institutional accountability for data privacy compliance; approves this policy and any material revisions; ensures adequate resources are allocated to the privacy Program
Vice President for Administration	Operationally responsible for privacy Program implementation; appoints the Privacy Officer; receives quarterly privacy compliance reports; approves the AIU Privacy Notice
Privacy Officer	Develops and maintains the privacy Program; advises on data protection compliance; responds to data subject requests; investigates data incidents; maintains the Data Processing Register; delivers privacy training; monitors compliance; reports to the VP Administration; serves as the primary contact for data subjects and regulators
Data Stewards (IR Director, Registrar, HR Director, IT Director, Deans)	Responsible for the accuracy, security, and appropriate use of personal data within their domain; implement privacy controls; report data incidents to the Privacy Officer; respond to data subject requests within their domain within 5 working days of referral from the Privacy Officer
IT Department	Implements and maintains the technical security measures protecting personal data; manages access controls and data systems; supports data breach detection and response; implements data retention and destruction schedules
Faculty Members	Obtain required ethics approval before collecting student or participant personal data for research; use minimum necessary data; protect data collected in the course of teaching and supervision; report suspected incidents to the Privacy Officer
All Employees and Contractors	Handle personal data only within the scope of their role; not disclose personal data to unauthorised parties; complete required privacy training;

 AMERICAN INTERNATIONAL UNIVERSITY الجامعة الأمريكية الدولية	Policy Main Title	Privacy and Personal Data Protection Policy	Effective Date	14/06/2026
	Category	Administration and Campus Operations	Last Review date	
	Policy Number	ADM-002	Next Review date	14/06/2029
	Responsible Entity	VP Administration	Approved By	President

	report suspected incidents or breaches immediately to their supervisor and the Privacy Officer
Human Resources Department	Ensures employee data is collected, processed, and stored in accordance with this policy and Kuwait Labour Law; manages employee data subject requests; maintains employee data retention and disposal schedules

Article 11: Privacy Governance

11.1 Privacy Officer

The Privacy Officer is appointed by the VP Administration from among qualified AIU staff or through an external appointment. The Privacy Officer has sufficient seniority, resources, and institutional access to fulfil this role effectively and independently. The Privacy Officer attends senior leadership meetings where data privacy matters are discussed and has direct access to the VP Administration and, where the matter warrants it, the President.

11.2 Data Processing Register

The Privacy Officer maintains the Data Processing Register, a comprehensive, current record of all categories of personal data processed by AIU. The Register is updated: when a new data collection activity begins; when an existing activity is modified; when a retention period expires and data is disposed of; and annually as part of the privacy Program review. The Register is made available to Accrediting agency visiting teams and to any Kuwait regulatory authority with jurisdiction upon request.

11.3 Privacy Training

All AIU employees and contractors with access to personal data complete privacy training before being granted data access and annually thereafter. Training covers: the principles of this policy; the employee's specific data-handling obligations; the data subject rights and the procedure for handling data subject requests; how to identify and report a data incident; and the consequences of privacy policy violations. Training completion is tracked by HR and reported to the Privacy Officer quarterly. An employee whose training has lapsed may not have access to sensitive personal data systems until training is renewed.

11.4 Annual Privacy Review

The Privacy Officer conducts an annual review of AIU's privacy Program, covering: compliance with this policy across all departments; the Data Processing Register currency; the status of data subject requests and complaints; incidents and their resolution; training compliance; and any changes in Kuwait law or accreditation requirements affecting privacy obligations. The annual review report is presented to the VP

 AMERICAN INTERNATIONAL UNIVERSITY الجامعة الأمريكية الدولية	Policy Main Title	Privacy and Personal Data Protection Policy	Effective Date	14/06/2026
	Category	Administration and Campus Operations	Last Review date	
	Policy Number	ADM-002	Next Review date	14/06/2029
	Responsible Entity	VP Administration	Approved By	President

Administration and the Board Audit and Risk Committee. Findings and remediation plans are incorporated into the following year's privacy Program priorities.

Article 12: Violations and Consequences

- Employees who handle personal data in violation of this policy, including unauthorized disclosure, failure to report an incident, or processing data for purposes not authorized by this policy, are subject to disciplinary action under the applicable employment policy, up to and including termination.
- Where a violation constitutes a breach of Kuwait law, the matter is referred to the VP Administration and Legal Counsel for assessment of regulatory and legal liability.
- Students who access or disclose another person's personal data without authorization in the context of an AIU activity are subject to disciplinary action under the AIU Student Conduct Policy.
- Third-party providers who breach their data processing agreement are subject to contractual remedies and, where the breach has caused harm to individuals, may face legal action.
- Retaliation against any person who reports a suspected privacy violation or data incident in good faith is prohibited and is subject to the protections of GOV-003 (Whistleblower Protection Policy).

Procedures

Responding to a Data Subject Request

- The data subject submits a written request to the Privacy Officer by email or through the Data Subject Request Form available on the AIU website. The request identifies the data subject, the nature of the right being exercised (access, correction, erasure, portability, objection), and any additional context.
- The Privacy Officer acknowledges receipt within 3 working days and confirms the data subject's identity where necessary to prevent fraudulent requests. The Privacy Officer logs the request in the Data Subject Request Register.
- The Privacy Officer consults with the relevant data steward(s) to gather the information or confirm the action required. Data stewards respond to Privacy Officer requests within 5 working days.
- The Privacy Officer issues a substantive response to the data subject within 30 calendar days of receipt. Where the request is complex or involves multiple data domains, the Privacy Officer may extend by a further 30 days with written notice to the data subject before the original deadline.
- Where the request is declined, because a legal retention obligation prevents erasure, because the data is needed to perform a contract, or for another valid reason, the Privacy Officer communicates the grounds in writing and informs the data subject of their right to escalate to the VP Administration or to the relevant regulatory authority.

 AMERICAN INTERNATIONAL UNIVERSITY الجامعة الأمريكية الدولية	Policy Main Title	Privacy and Personal Data Protection Policy	Effective Date	14/06/2026
	Category	Administration and Campus Operations	Last Review date	
	Policy Number	ADM-002	Next Review date	14/06/2029
	Responsible Entity	VP Administration	Approved By	President

Reporting and Managing a Data Incident

1. Any employee who discovers or suspects a data incident immediately notifies their supervisor and the Privacy Officer, by phone for urgent matters, followed by written notification within 1 working day. The notification states: what happened; the data and individuals potentially affected; the immediate action taken; and whether the incident is ongoing.
2. The Privacy Officer assesses the severity of the incident within 2 hours of notification and initiates the appropriate response level from the incident response table in Article 8. Where the incident may be High severity, the VP Administration and President are notified immediately.
3. The Privacy Officer leads the incident investigation, working with IT, HR, the relevant data steward, and Legal Counsel as appropriate. The investigation establishes: the cause; the data affected; the individuals affected; the extent of potential harm; and the corrective action required.
4. Where notification to affected data subjects is required, because the incident poses a high risk to their rights or interests, the Privacy Officer prepares a notification letter for VP Administration approval and issues it within the timeframe required. Notifications are clear, honest, and include what happened, what AIU is doing about it, and what the data subject should do to protect themselves.
5. The Privacy Officer closes the incident record in the Data Incident Register when all corrective actions are confirmed complete. The incident is reported in aggregate form (without identifying individual staff involved) in the quarterly privacy report to the VP Administration and the annual report to the Board Audit and Risk Committee.

Annual Privacy Program Review

1. By 1 October each year, the Privacy Officer initiates the annual privacy Program review, compiling: the Data Processing Register (current version); the year's data subject request log; the year's incident log; training completion rates by department; any changes in Kuwait law or accreditation requirements since the last review; and any third-party security assessments received.
2. The Privacy Officer reviews each department's compliance with this policy through a self-assessment questionnaire distributed to all data stewards. Data stewards return completed assessments by 31 October. The Privacy Officer summarizes findings and identifies departments or data processes with compliance gaps.
3. The Privacy Officer prepares the Annual Privacy Program Review Report by 30 November, covering: the overall compliance status; specific findings by department or data category; the year's incidents and their root causes; data subject request performance; training compliance; and recommendations for the following year.
4. The Report is presented to the VP Administration for review and endorsement. The VP Administration presents the Report summary to the Board Audit and Risk Committee at its next meeting. Material findings requiring Board action are escalated immediately.
5. The Privacy Officer incorporates the Review findings into an updated Data Processing Register, a revised training Program where deficiencies are identified, and a compliance action plan for the following year with named responsible officers and deadlines.

 AMERICAN INTERNATIONAL UNIVERSITY الجامعة الأمريكية الدولية	Policy Main Title	Privacy and Personal Data Protection Policy	Effective Date	14/06/2026
	Category	Administration and Campus Operations	Last Review date	
	Policy Number	ADM-002	Next Review date	14/06/2029
	Responsible Entity	VP Administration	Approved By	President

President Signature

Signature: _____ Date: _____