INTERNATIONAL ASSOCIATION OF PRIVATE UNIVERSITIES AND COLLEGES

Part Nine: IAPUC Digital Security and Privacy Regulations

Document No.: IAPUC/IQA/DSP-2026-001

Version: 1.0

Effective Date: Pending Official Release

Formulated by: IAPUC Quality Accreditation Committee

Applicable Recipients: Global private universities, private colleges and private higher vocational education institutions applying for or maintaining IAPUC-IQA accreditation, as well as all experts and staff participating in accreditation review work

Preface

In an era where digital technologies are deeply integrated into higher education, digital security and privacy protection have become indispensable and critical dimensions for measuring school-running quality. The collection, storage, transmission and processing of information run through every link of enrollment, teaching, evaluation, research and institutional administration, accompanied by inherent risks of data leakage and abuse that pose substantial threats to the rights and interests of teachers and students, institutional reputation, and accreditation credibility.

When establishing the Internal Quality Assurance (IQA) system, the International Association of Private Universities and Colleges (IAPUC) incorporated "Resource and Support System" and "Ethics and Compliance" into the core standard domains. Digital security and privacy protection serve as the key intersection of these two standard domains — it constitutes both the digital infrastructure guarantee that institutions must provide and the basic commitment that institutions must fulfill in terms of ethics and social responsibility.

These Regulations aim to establish a clear and operable set of norms for digital security and privacy protection for accredited institutions and the accreditation review process. Integrating the core concepts of the ISO/IEC 27001 international information security management system, the data protection principles of the EU General Data Protection Regulation (GDPR), and best practices in the higher education sector, while fully considering the diversity of resource conditions and technical capabilities of private higher education institutions, these Regulations adhere to the mission-driven and continuous improvement-oriented accreditation philosophy. IAPUC firmly believes that academic quality in the digital era must be grounded in data dignity and secure trust.

Chapter 1 General Provisions

Article 1 Purposes and Objectives

These Regulations aim to:

(1) Establish the basic principles and minimum requirements for digital security and privacy protection within the IAPUC-IQA accreditation system;

(2) Provide normative guidelines for accredited institutions to build a digital security governance framework and privacy protection system;

(3) Standardize digital information processing behaviors in the accreditation review process to ensure institutional data security and confidentiality of review information;

(4) Enable accredited institutions to develop systematic capabilities for digital risk identification, prevention and emergency response.

Article 2 Scope of Application

These Regulations apply to:

(1) All private higher education institutions that have obtained or are applying for IAPUC-IQA accreditation (hereinafter referred to as "Accredited Institutions");

(2) All digital information processing activities of Accredited Institutions in the entire school-running process, including but not limited to student personal data, faculty personnel information, academic research data, financial and donation information, teaching quality evaluation data, as well as data of institutional management information systems and online teaching platforms;

(3) The access, storage and processing of institutional digital information by the IAPUC Quality Accreditation Committee, IQA Office, peer review experts, members of the Accreditation Decision Committee, and members of the Appeal and Arbitration Committee during the accreditation review process.

Article 3 Core Principles

The IAPUC-IQA digital security and privacy protection system implements the following seven core principles:

Principle	**Core Connotation**
Legitimacy, Fairness and Transparency	Personal data processing must be based on legitimate grounds, and the purposes and methods of processing shall be transparently notified to data subjects.
Purpose Limitation	Data collection shall be for specific, explicit and legitimate purposes, and no further processing shall be conducted in a manner inconsistent with such purposes.
Data Minimization	Collected personal data shall be necessary, appropriate and non-excessive for the processing purposes.
Accuracy	Personal data shall be kept accurate and up-to-date, and inaccurate personal data shall be erased or corrected in a timely manner.
Storage Limitation	Personal data shall not be stored for a period longer than necessary for the processing purposes.
Integrity and Confidentiality	Data processing shall ensure an appropriate level of security, including protection against unauthorized or illegal processing, as well as accidental loss, damage or destruction

	of data.
Accountability	Data controllers shall be accountable for complying with the above principles and shall be able to demonstrate compliance.

The above seven principles are closely aligned with the core values of IAPUC-IQA, namely "Rigor", "Fairness", "Transparency" and "Social Responsibility", and serve as the basic evaluation criteria for the digital governance capabilities of Accredited Institutions.

Chapter 2 Institutional Digital Security Governance

Article 4 Digital Security Governance Framework

Accredited Institutions shall establish a university-wide digital security governance framework with clear rights and responsibilities allocated from the top management level to the executive level.

Leadership Responsibility

The chief administrative officer of the institution (president or equivalent position) shall bear the ultimate responsibility for digital security and privacy protection. The institution shall appoint a digital security officer (such as Chief Information Security Officer or equivalent role) from the top management to oversee the overall digital security work of the institution.

Full-time Institutions or Posts

In accordance with its own scale and risk characteristics, the institution shall set up a full-time digital security management institution or clarify the security management responsibilities of the existing information technology department. Such institution or post shall undertake the following core functions:

Formulate and update digital security and privacy protection policies;

Organize digital security risk assessments and internal audits;

Manage the monitoring, response and reporting of information security incidents;

Coordinate university-wide digital security training and awareness education.

System Construction

Institutions shall formulate and publicly release the following core institutional documents:

Digital Security Policy;

Personal Data Protection Policy (Privacy Policy);

Acceptable Use Policy for Information Systems;

Information Security Incident Emergency Response Procedures;

Third-Party Data Processing Agreement Template.

Article 5 Digital Security Risk Management

Accredited Institutions shall establish a systematic digital security risk management mechanism.

Asset Identification and Classification

Institutions shall identify and register key information assets, including but not limited to student information systems, learning management systems, research databases, financial systems, personnel file systems and email systems, and classify and grade such assets based on their importance and sensitivity.

Risk Assessment

Institutions shall conduct security risk assessments on key information assets regularly (at least once every two years), covering threat identification, vulnerability analysis, impact assessment and risk level determination. The scope of risk assessment shall include technical risks, management risks and human-induced risks.

Risk Treatment

Institutions shall formulate risk treatment plans based on risk assessment results, clarifying treatment strategies (avoidance, mitigation, transfer or acceptance) and their implementation schedules. Treatment measures for high-risk items shall be initiated within 6 months upon completion of the risk assessment and continuously tracked until risk reduction is achieved.

Third-Party Management

When cooperating with third-party service providers involved in data processing (such as cloud platforms, learning management system suppliers and enrollment agency platforms), institutions shall:

Evaluate the security capabilities of third parties;

Specify the scope, purpose, security requirements and compliance obligations of data processing in contracts;

Conduct regular supervision on third-party data processing activities.

Article 6 Data Lifecycle Management

Accredited Institutions shall implement full lifecycle management of personal data.

Lifecycle Stage	Management Requirements
Collection	Clarify collection purposes and legal bases, provide data subjects with clear and readable privacy notifications, and obtain necessary consent where consent serves as the processing basis.
Storage	Implement access control management, ensure the security of data storage devices, and adopt graded storage and encryption protection for data of different sensitivity levels.
Usage	Use data within the declared purposes, establish a data usage approval system, and record logs for bulk data usage.
Sharing and Transmission	Clarify the scope, conditions and security measures for data sharing, and assess the data protection level of recipients for cross-border data transmission.
Archiving	Distinguish between active data and archived data, implement hierarchical management, and ensure the long-term readability and integrity of archived data.
Destruction	Implement irreversible secure destruction (such as secure erasure or physical destruction) upon the expiration of the data storage period.

Article 7 Technical Security Measures

Accredited Institutions shall deploy technical security measures commensurate with their scale and risk levels. These Regulations do not specify specific technical solutions, but institutions shall demonstrate that they have covered the following security capability domains and adopted reasonable measures:

Access Control

Implement identity-based access control in compliance with the principle of least privilege;

Strengthen the management and regular audit of privileged accounts (e.g., system administrators);

Realize role separation to prevent excessive control of key systems by a single individual.

Encryption Protection

Encrypt sensitive personal data at rest and in transmission;

Securely manage encryption keys separately from encrypted data.

Network Security

Deploy boundary protection measures (e.g., firewalls, intrusion detection and prevention systems);

Implement multi-factor authentication for remote access;

Conduct regular penetration testing or vulnerability scanning.

System Security

Establish systematic patch management and vulnerability remediation procedures;

Incorporate security requirements into design (shift-left security) during the development or procurement of information systems;

Implement unified security baseline management for terminal devices.

Log and Monitoring

Record audit logs for access and operations of key systems with a log retention period of no less than 12 months;

Establish a security incident monitoring mechanism to ensure timely detection of abnormal behaviors.

Backup and Recovery

Implement regular automatic backup of key business data;

Store backup data in storage media physically isolated from original data;

Conduct regular backup and recovery drills to ensure the reliability of recovery procedures.

Physical and Environmental Security

Implement physical access control for key facilities such as computer rooms and data centers;

Deploy environmental monitoring measures (temperature and humidity, power supply, fire protection, etc.).

Chapter 3 Privacy Protection Specifications

Article 8 Student Personal Data Protection

Student personal data during schooling is one of the most sensitive data assets of Accredited Institutions. Institutions shall meet the following requirements for student personal data protection:

Legitimate Processing Grounds

Institutions must have explicit legal grounds for processing student personal data. Common legitimate grounds between institutions and students include:

Necessity for the performance of educational contracts (e.g., student status management, grade recording, degree awarding);

Statutory obligations undertaken by institutions (e.g., submitting data to competent educational authorities);

Explicit consent from students (where no other legitimate grounds apply).

Special Category Data Protection

Special category data such as race, religious belief, health status and biometric information shall be subject to enhanced protection. Prior to processing such data, institutions shall obtain explicit consent from students or prove that the processing is necessary to protect the major interests of students.

Student Right to Know

At or before the collection of student personal data, institutions shall provide students with privacy notifications in concise and understandable language, covering at least the following contents:

Identity and contact information of the data controller;

Processing purposes and legal bases;

Categories of data recipients;

Data storage period;

Personal data rights of students and the ways to exercise such rights.

Protection of Student Rights

Institutions shall establish mechanisms to guarantee students' exercise of the following data rights:

Right of Access: To inspect their personal data;

Right of Rectification: To request the correction of inaccurate personal data;

Right of Erasure: To request the erasure of personal data under statutory circumstances;

Right of Restriction of Processing: To request the restriction of data processing under specific circumstances;

Right of Data Portability: To obtain personal data provided by themselves in a structured and machine-readable format (applicable to automated processing based on consent or contract).

Data Breach Notification

In the event of a personal data breach that poses a high risk to the rights and freedoms of students, institutions shall notify the affected students within 72 hours upon discovery (except for statutory exemptions), and report to relevant regulatory authorities when necessary. The notification shall include the nature of the breach, potential impacts, and remedial measures taken and recommended.

Article 9 Faculty and Staff Data Protection

The core principles applicable to student data protection shall apply to the personal data protection of faculty and staff. In addition, institutions shall pay special attention to the following requirements:

The confidentiality of faculty personnel files and performance evaluation data shall be strictly restricted to authorized management personnel;

The storage and usage of faculty academic achievements and relevant evaluation data shall comply with both privacy and intellectual property norms;

Prior to the deployment of staff monitoring (e.g., email monitoring, network behavior monitoring), institutions shall conduct necessity and proportionality assessments and fully inform staff.

Article 10 Research Data and Participant Privacy

Accredited Institutions shall protect the privacy rights and interests of research participants in academic research activities:

For research projects involving human participants, privacy protection measures shall be incorporated into the research proposal and approved by the Ethics Review Committee prior to project initiation (see *IAPUC-IQA Academic Ethics and Code of Conduct*);

Research data shall be anonymized or pseudonymized to the maximum extent possible;

No personally identifiable information of participants shall be disclosed in the publication of research results unless explicit consent is obtained from the participants;

Research involving special groups (e.g., minors, persons with disabilities, prisoners)

shall be equipped with dedicated risk assessment and privacy protection plans.

Article 11 Cross-Border Data Transmission

When conducting cross-border transmission of personal data (including providing data to overseas service providers or allowing access by overseas entities), Accredited Institutions shall:

Record the legitimate grounds, purposes and security measures for data transmission;

Evaluate the data protection legal environment of the recipient country or region to ensure that the post-transmission data protection level is not substantially lower than the standards of the institution’s home country;

Sign data transmission agreements containing appropriate protection clauses with data recipients;

Inform data subjects of the occurrence and potential risks of cross-border data transmission.

Chapter 4 Application of Digital Security and Privacy Protection in Educational Technology

Article 12 Learning Management Systems and Online Teaching Platforms

Accredited Institutions shall comply with the following norms in the use of learning management systems and online teaching platforms:

Take security and privacy protection capabilities as core evaluation indicators during platform selection;

Conduct security assessment and privacy impact assessment before platform launch;

Formulate clear internal norms for the management and usage of student learning behavior data stored on platforms (e.g., login records, learning duration, assignment submission, discussion participation), and restrict access rights and usage purposes;

The application of learning analytics shall be oriented to promoting student learning, and students shall be fully informed of its purposes, data scope and potential impacts prior to application.

Article 13 Application of Educational Artificial Intelligence

When researching or deploying artificial intelligence technologies to assist teaching evaluation, academic early warning or personalized learning, Accredited Institutions

shall:

Ensure that the decision-making logic of AI systems is interpretable, and no unappealable automated decisions are made for students;

Review the source legality and unbiasedness of training data used by AI systems;

Inform students of the nature and extent of AI tool participation in academic evaluation or guidance;

AI-assisted evaluation results shall be reviewed by teachers before being adopted as formal academic judgments.

Article 14 Distance Education and Virtual Learning Environments

Accredited Institutions providing distance education or blended teaching shall pay additional attention to the following requirements:

The use of online examination proctoring tools shall balance privacy intrusion and academic integrity guarantee, and the proctoring methods, collected data and storage period shall be explained to students in advance;

Informed consent from students shall be obtained when student portraits or voices are involved in course recordings;

Teacher-student interaction data in virtual learning environments shall be managed separately from other administrative data.

Chapter 5 Digital Security and Confidentiality in Accreditation Review

Article 15 Information Management in the Review Process

Information generated during the IAPUC-IQA accreditation review process shall be subject to strict security and confidentiality systems.

Protection of Institutional Materials

Self-evaluation reports, evidence materials and supplementary explanations submitted by institutions shall be stored and managed by the IQA Office in a controlled encrypted environment;

Access rights to review materials shall be limited to experts and staff directly participating in the corresponding review case;

Accreditation archives shall be retained for 10 years after the expiration of the accreditation term and securely destroyed upon expiry.

Review Platform Security

If IAPUC adopts an online platform for material submission and review, the platform shall implement transmission encryption, access control and audit log recording;

The platform shall pass independent security assessment before official operation.

Remote Communication Security

Remote meetings and online interviews during the review process shall adopt communication tools with end-to-end encryption;

Remote meeting recordings shall only be made with informed consent from all participants, and the security management of recording files shall be consistent with that of written review materials.

Article 16 Confidentiality Obligations of Experts and Staff

All experts and staff participating in accreditation review shall sign a *Confidentiality Commitment Letter* before taking office, undertaking unlimited confidentiality obligations for non-public institutional information accessed during the review process.

Review experts shall not store non-public accreditation documents on personal devices, and shall securely return or destroy relevant materials upon completion of work.

Confidentiality obligations survive the termination of review tasks, invalidation of expert qualifications or termination of employment relationships.

Article 17 Information Security Incident Response

In the event of an information security incident that may affect the confidentiality of accreditation review materials or the security of IAPUC information systems, the IQA Office shall initiate the emergency response procedure within 24 hours upon discovery.

If the security incident involves materials submitted by accredited institutions, the IQA Office shall notify the affected institutions within 72 hours after confirmation, explaining the nature of the incident, potential impacts and adopted measures.

The IQA Office shall compile records of information security incidents and incorporate them into the internal quality review archives of the accreditation system.

Chapter 6 Supervision, Evaluation and Continuous Improvement

Article 18 Institutional Self-Evaluation Requirements

Accredited Institutions shall incorporate digital security and privacy protection into the annual quality monitoring report required by the *IAPUC-IQA Accreditation Manual*, covering at least the following contents:

Summary of annual digital security risk assessment results;

Statistics of annual information security incidents (aggregated data with privacy protection) and explanations of major incidents;

Implementation status of privacy impact assessments;

Coverage and effectiveness of digital security training;

Updates to policies and systems.

Article 19 Digital Security Review in Accreditation Evaluation

During the desk review and on-site visit stages of accreditation review, peer review experts shall incorporate the institutional digital security and privacy protection status into the review scope, evaluating its compliance with IAPUC-IQA accreditation standards (Standard 6 "Resource and Support System" and Standard 1 "Ethics and Compliance").

Key review priorities include:

Completeness of the digital security governance framework and system construction;

Operational effectiveness of the digital security risk management mechanism;

Implementation of student personal data protection systems and rights guarantee mechanisms;

Adequacy of information security incident response capabilities.

If the review identifies major deficiencies in institutional digital security or privacy protection (such as massive student data leakage or absence of basic access control), such findings may serve as an important basis for granting provisional accreditation or denying accreditation.

Article 20 Continuous Improvement

IAPUC encourages Accredited Institutions to regard digital security and privacy protection as a dynamically optimized process and continuously improve their digital governance capabilities in accordance with the PDCA cycle.

The Digital Security Standards Working Group will regularly track the development of international digital security regulations and best practices, and put forward revision suggestions for these Regulations to the Quality Accreditation Committee when necessary.

IAPUC will issue best practice guidelines for digital security and privacy protection from time to time to provide learning references and benchmarking standards for Accredited Institutions.

Chapter 7 Supplementary Provisions

Article 21 Term Definition

Term	Definition
Personal Data	Any information relating to an identified or identifiable natural person (data subject).
Data Processing	Any operation or set of operations performed upon personal data, including collection, recording, storage, usage, transmission, disclosure, erasure, etc.
Data Controller	An entity that determines the purposes and means of personal data processing independently or jointly with others — in the institutional context, it generally refers to the institution itself.
Data Subject	A natural person to whom personal data refers — in the institutional context, generally students, faculty and staff.
Privacy Impact Assessment	A systematic process of assessing the privacy impacts and determining mitigation measures prior to initiating high-risk personal data processing activities.
Information Asset	Information or information systems in electronic or paper form that are valuable to the institution.
Information Security Incident	Any unexpected event that may adversely affect the confidentiality, integrity or availability of information assets.
Personal Data Breach	A security incident resulting in accidental or illegal destruction, loss, alteration, unauthorized disclosure or access to personal data.

Article 22 Relationship with Other Normative Documents

These Regulations and the following documents constitute the unified IAPUC-IQA

normative system:

Document	Relationship with These Regulations
IAPUC-IQA Accreditation Manual	These Regulations refine the information infrastructure security requirements under Standard 6 "Resource and Support System" and extend the "Ethics and Compliance" Standard 1 to the digital domain.
IAPUC-IQA Academic Certification Quality Standards Manual	These Regulations provide security baselines for academic information management, learning outcome evaluation data storage and faculty-student digital environment governance.
IAPUC-IQA Accreditation Process Specification	These Regulations provide normative support for information confidentiality and data security throughout the entire accreditation review process.
IAPUC-IQA Academic Ethics and Code of Conduct	These Regulations complement the ethical specification in terms of data ethics, research participant privacy protection and integrity obligations.

Article 23 Specification Interpretation and Revision

These Regulations are interpreted by the IAPUC Quality Accreditation Committee.

IAPUC reserves the right to revise these Regulations in accordance with the development of digital security laws and regulations and accreditation practices. Revised versions shall be released upon approval by the IAPUC Council with an appropriate transition period.

Upon the entry into force of these Regulations, institutions applying for accreditation and new applicants shall achieve compliance gradually from the date of obtaining candidate qualification or the effective date of these Regulations (whichever is later). Already accredited institutions shall elaborate their compliance progress in the first annual report after the implementation of these Regulations.

Article 24 Entry into Force

These Regulations shall come into force on the date of approval by the IAPUC Council.

Appendix: Digital Security and Privacy Protection Self-Evaluation Checklist

Institutions may conduct preliminary self-evaluation of digital security and privacy

protection using the following checklist:

Dimension	Core Evaluation Questions	Yes/Partially/No	Improvement Actions Required
Leadership Responsibility	Has a digital security officer at the top management level been appointed?		
System Construction	Have formal digital security policies and privacy protection policies been formulated?		
Asset Identification	Has the identification and classification of key information assets been completed?		
Risk Assessment	Has a formal digital security risk assessment been conducted within the past two years?		
Access Control	Is access control implemented in compliance with the principle of least privilege?		
Encryption Protection	Is encryption applied to sensitive data at rest and in transmission?		
Log Audit	Do key systems enable and		

	properly retain audit logs?		
Backup and Recovery	Is a regular data backup and recovery drill mechanism established?		
Third-Party Management	Are third-party service providers involved in data processing subject to security assessment and contractual constraints?		
Privacy Notification	Do students receive clear privacy notifications prior to data collection?		
Student Rights Protection	Is a mechanism established to accept and respond to student requests for exercising data rights?		
Breach Response	Is an emergency response procedure established for information security incidents and personal data breaches?		
Security Training	Is regular digital security and privacy protection training conducted		

	for all faculty, staff and students?		
Learning Platform Security	Have learning management systems and online teaching platforms undergone security assessment?		
AI Application Governance	If AI is applied in assisted teaching or assessment, is a corresponding ethical and privacy review mechanism established?		

Document Approval

Role	Name/Position	Date
Compiled by	IAPUC Quality Accreditation Committee Digital Security Standards Working Group	May 2026
Reviewed by	IAPUC Quality Accreditation Committee	Pending
Approved by	IAPUC Council	Pending

Copyright Statement