INTERNATIONAL ASSOCIATION OF PRIVATE UNIVERSITIES AND COLLEGES

Part XVII: IQA Accreditation Records and Data Retention Management Rules

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

Version: 1.0

Effective Date: Pending Official Release

Formulating Institution: IAPUC Quality Accreditation Committee, International Association of Private Universities and Colleges

Applicable Scope: The IQA Office, peer review experts, members of the Accreditation Decision Body, members of the Appeals and Arbitration Committee, and all private higher education institutions applying for or holding valid IQA accreditation

Preface

Accreditation records serve as the institutional memory of the credibility of the IAPUC-IQA accreditation system. Every self-evaluation report, every review record, and every decision-making process not only documents the quality pursuit trajectory of accredited institutions but also forms the cornerstone of the transparency and traceability of the accreditation system. The massive volume of data and records generated in accreditation activities are public assets that safeguard the right to know of stakeholders, while also bearing the legitimate rights, interests and privacy expectations of institutions, teachers, students and review experts. Achieving a balance between **long-term retention for traceability** and **regular cleanup for risk reduction**, and safeguarding the integrity and security of records while respecting the rights of data subjects, constitute the core issues that must be addressed by accreditation record management.

Formulated to establish a full lifecycle management specification covering the generation, filing, preservation, utilization and final destruction of all records and data generated from IQA accreditation activities, these Rules adopt the core design principles of **classified management, graded protection, full-process traceability and scheduled cleanup**. Closely aligned with the *IAPUC Digital Security and Privacy Regulations* and the *IAPUC-IQA Academic Ethics and Code of Conduct*, these Rules jointly build the information governance defense line of the IQA accreditation system.

Chapter I General Provisions

Article 1 Purposes and Basis

These Rules are formulated for the following purposes:

(1) To define the scope, types and ownership of IQA accreditation records and data;

(2) To establish a classified retention term system based on the sensitivity and business value of records, ensuring compliant retention and scheduled cleanup of records;

(3) To formulate unified safety management standards for the storage, access, transmission and destruction of records;

(4) To balance the relationship between record utilization and confidentiality protection, and respect the legitimate rights and interests of data subjects;

(5) To clarify the cooperation obligations of accredited institutions in accreditation record management.

These Rules are formulated based on:

- Provisions on data lifecycle management and technical security measures stipulated in the *IAPUC Digital Security and Privacy Regulations*;

- Provisions on document submission and confidentiality obligations at all stages of

accreditation specified in the *IAPUC-IQA Accreditation Procedure Specifications*;

- Requirements for case record management stipulated in the *IQA Accreditation Appeals, Complaints and Dispute Resolution Management Measures*;

- General Principles for Archives Management issued by the International Council on Archives (ICA);

- ISO 15489-1:2016 Information and Documentation — Records Management Standard.

Article 2 Scope of Application

These Rules shall apply to:

(1) All records and data generated or received by the IQA Office in the course of accreditation management activities;

(2) All records and data generated or accessed by peer review experts, members of the Accreditation Decision Committee, and members of the Appeals and Arbitration Committee in accreditation-related activities;

(3) All accreditation-related documents submitted by accredited institutions and derived review and decision documents;

(4) All official accreditation-related records retained by accredited institutions themselves.

Article 3 Basic Principles

The management of IQA accreditation records shall adhere to the following basic principles:

Principle	**Core Connotation**
Integrity	A complete record chain shall be formed throughout the entire accreditation process to ensure traceability and auditability of decision-making procedures.
Security	Matching security protection measures shall be adopted for the storage, transmission and access of records based on their sensitivity level.
Minimum Retention	Records shall not be retained longer than necessary for business operations and legal compliance obligations, and shall be destroyed in accordance with regulations upon expiration.
Traceability	All operations including record access, authorized modification and destruction shall be fully documented to form tamper-proof audit logs.

Clear Rights and Obligations	The rights and responsibilities of record generators, managers, users and destruction approvers shall be clearly defined and implemented by respective parties.

Chapter II Classification and Scope of Records

Article 4 Record Classification

Based on business sources and information attributes, IQA accreditation records are divided into five categories as follows:

(1) Institutional Accreditation Records

Records submitted by accredited institutions and generated by IQA in institutional accreditation activities, including:

1. Accreditation application documents and qualification review materials;

2. Self-evaluation reports and all supporting evidence materials;

3. Annual quality monitoring reports and interim self-evaluation briefings;

4. Major institutional change reports and relevant handling records;

5. Quality representative appointment letters, change records and communication archives;

6. Accreditation fee payment and financial transaction records;

7. Accreditation certificate issuance and accreditation status publicity records;

8. Archived copies of institutional annual information disclosure documents (versions archived by the IQA Office).

(2) Review and Decision Records

Records generated during accreditation review and decision-making processes, including:

1. Peer review panel formation and appointment records;

2. Conflict of interest declarations and confidentiality commitments of review experts;

3. Desk review working papers and issue lists;

4. On-site visit records — including interview summaries, facility inspection records and evidence verification records (excluding original personal privacy notes of review experts, with only official summaries compiled and submitted in accordance with panel resolutions retained);

5. Peer review reports and panel members’ opinions (including minority opinions);

6. Institutional response opinions on review reports;

7. Meeting minutes and voting records of the Accreditation Decision Committee;

8. Accreditation decision notices.

(3) Appeal, Complaint and Dispute Resolution Records

Records generated in the process of appeal, complaint and dispute resolution, including:

1. Appeal letters, complaint letters and dispute mediation applications;

2. Case filing review and investigation records;

3. Working records and reports of review panels and investigation teams;

4. Hearing records (if applicable);

5. Rulings, handling decisions and settlement agreements;

6. Whistleblower protection records.

(4) Expert and Personnel Management Records

Records generated in the management of peer review experts and IQA staff, including:

1. Expert database application/recommendation forms, review records and appointment certificates;

2. Expert training and assessment records;

3. Expert evaluation and promotion records;

4. Expert violation investigation and disposal records;

5. Expert exit records;

6. Performance and compliance records of IQA Office staff;

7. Confidentiality commitment signing records.

(5) Financial and Administrative Records

Records generated in IQA accreditation financial and administrative management, including:

1. Annual budget and final accounts documents;

2. Audit reports and response documents to management suggestions;

3. Formulation and adjustment records of charging standards;

4. Revenue and expenditure vouchers and accounting books;

5. Contracts and agreement documents.

Article 5 Record Carrier Forms

IQA accreditation records include the following carrier forms:

(1) **Electronic Records**: Records generated, transmitted and stored in electronic form, including documents, spreadsheets, database records, emails, meeting audio and video recordings, video conference files and system logs in the electronic

accreditation platform;

(2) **Paper Records**: Original or copied documents preserved in paper form;

(3) **Mixed Records**: Records of the same business matter existing in both electronic and paper carriers. Associated indexes shall be established in the record management system to ensure mutual queryability of dual-track records.

Article 6 Filing Scope and Responsible Persons

(1) All official documents submitted by accredited institutions shall be filed immediately by the IQA Office upon receipt.

(2) Upon completion of review tasks, the panel leader shall organize and file review working papers (official archived versions only), official on-site visit summaries and review reports to the IQA Office within 30 days after submission.

(3) Meeting minutes and voting records of the Accreditation Decision Committee shall be filed by the committee secretary within 15 days after decision-making completion.

(4) All case materials of the Appeals and Arbitration Committee shall be filed by the committee secretary within 30 days after case closure.

(5) Financial records shall be filed within 60 days after the completion of annual financial audit by fiscal year.

(6) The IQA Office shall appoint dedicated record management personnel responsible for the daily management of record receipt, classification, cataloging, preservation and destruction.

Chapter III Retention Periods

Article 7 Principles for Setting Retention Periods

Record retention periods shall be comprehensively determined based on the following factors:

(1) The business reference value of records for current and future accreditation activities;

(2) The traceability requirements for potential appeals, complaints or legal disputes;

(3) Statutory retention requirements for financial and legal compliance;

(4) Information sensitivity of records — the retention period of highly sensitive personal data shall be shortened as much as possible on the premise of meeting business and legal requirements.

Article 8 Retention Period Schedule

Record	Record Content	Retention	Commencem

Category		Period	ent Date
Permanent Retention	Final accreditation decision records (including voting results) of the Accreditation Decision Committee	Permanent	Effective date of the decision
Permanent Retention	Official accreditation certificate issuance records and accreditation status history records	Permanent	Effective date of initial accreditation
Permanent Retention	Historical versions of accreditation standards, manuals and major normative documents	Permanent	Effective date of the version
Long-term Retention	Institutional self-evaluation reports and supporting materials (accredited institutions)	15 years after the expiration of the accreditation term	Expiration date of the accreditation term
Long-term Retention	Peer review reports and institutional response opinions	15 years after the expiration of the accreditation term	Expiration date of the accreditation term
Long-term Retention	Rulings of appeal and arbitration cases	15 years after case closure	Case closure date
Medium-term Retention	Institutional self-evaluation reports and supporting materials (non-accredited institutions)	10 years after the effective date of non-accreditation decision	Effective date of the decision
Medium-term Retention	Annual quality monitoring reports	10 years after submission	Submission date
Medium-term Retention	Major institutional change reports and handling records	10 years after submission	Submission date
Medium-term	Complete appeal and complaint case materials (excluding	10 years after case closure	Case closure date

Retention	rulings)		
Medium-term Retention	Review expert records (including database admission, evaluation, violation disposal and exit records)	10 years after expert exit	Expert exit date
Medium-term Retention	Financial records – budgets, final accounts and audit reports	10 years after audit completion	Issuance date of audit reports
Standard Retention	Qualification review materials (including informal communication records)	5 years after decision-making	Effective date of the decision
Standard Retention	Desk review working papers and issue lists	5 years after review completion	Submission date of review reports
Standard Retention	Conflict of interest declarations and confidentiality commitments of review experts	5 years after review task completion	Submission date of review reports
Standard Retention	On-site visit interview summaries and evidence verification records	5 years after review completion	Submission date of review reports
Standard Retention	Financial records – revenue and expenditure vouchers, accounting vouchers	7 years after audit completion	Issuance date of audit reports
Standard Retention	Accreditation fee payment records	7 years after payment	Payment date
Short-term Retention	General administrative correspondence and informal communication records	3 years after communication conclusion	Communication conclusion date
Short-term Retention	Unfiled drafts, temporary notes and working documents	1 year after matter completion	Matter completion date

Article 9 Extension of Retention Periods

(1) The retention period of relevant records shall be automatically extended under the following circumstances:

1. If the records are involved in ongoing appeals, complaints or legal proceedings, the retention period shall be extended for 5 years after the final conclusion of the case and the exhaustion of all remedy channels;

2. If the records are involved in ongoing investigations or audits, the retention period shall be extended for 5 years after the completion of the investigation or audit;

3. If laws and regulations require extended retention, such provisions shall prevail.

(2) Dedicated record management personnel shall mark extended retention records in the record management system, specifying the extension reasons and new retention period.

Article 10 Institutional Self-record Retention

Accredited institutions shall formulate and implement internal accreditation record management systems in accordance with the retention period standards stipulated in these Rules. Institutions shall provide complete and valid accreditation records within the retention period during on-site visits or subsequent reviews conducted by IQA. If an institution is unable to continue retaining records due to relocation, merger, closure or other reasons, it shall notify the IQA Office 60 days in advance to negotiate record handover and disposal plans.

Chapter IV Storage and Security Management

Article 11 Electronic Record Storage

(1) All IQA electronic records shall be stored in the IAPUC designated and security-assessed accreditation management information system or controlled file servers.

(2) The following technical protection measures shall be implemented for electronic records:

1. Encrypted Storage: Records containing sensitive personal data shall be encrypted at the storage layer;

2. Redundant Backup: Key business records shall be automatically backed up daily, and general records shall be automatically backed up weekly; backup data shall be stored in storage media or independent cloud regions physically isolated from source data;

3. Backup Recovery Drills: Backup data recovery tests shall be conducted at least once a year to verify the integrity and availability of backups;

4. Tamper Resistance: Officially filed electronic records shall be set to read-only mode; any authorized modification shall be accompanied by complete modification logs and before-and-after version comparisons;

5. Format Management: Priority shall be given to storing records in open-standard or

long-term readable file formats to avoid unreadable records caused by software obsolescence.

(3) The integrity of electronic record storage media shall be verified regularly, and data migration shall be conducted timely for degraded media.

Article 12 Paper Record Storage

(1) Paper records shall be stored in dedicated archives or filing cabinets designated by the IQA Office, with environmental conditions complying with basic fireproof, moisture-proof, insect-proof and light-proof requirements.

(2) Highly sensitive paper records (e.g., documents containing large-scale personal student data) shall be locked and sealed for preservation, with access subject to approval by dedicated record management personnel.

(3) Long-term valuable paper records are encouraged to be digitally scanned and managed as electronic records with equivalent security standards. However, scanned copies shall not automatically replace the retention obligation of paper originals; originals shall still be retained in accordance with the periods specified in these Rules, unless retention of only digital copies is approved by the Director of the IQA Office.

Article 13 Access Control

(1) The access authority of IQA accreditation records shall be managed in accordance with the **minimum necessity principle**:

Record Category	**Access Authority**
Institutional accreditation applications and self-evaluation materials	Authorized IQA Office staff, review panel members of the relevant case, ADC members (during decision review period), and appeal review panel members (during appeal acceptance period)
Review reports and decision records	In addition to the above personnel, authorized academic researchers engaged in accreditation quality assurance research may access desensitized versions upon approval by the Director of the IQA Office
Institutional self-owned records	Institutions have the right to access all their submitted records and relevant review reports within the retention period
Appeal and complaint case files	Limited to members of the Appeals and Arbitration Committee, investigation team members and personnel authorized by the Director of the IQA Office

Financial records	Limited to IQA finance staff, treasurers, members of the IAPUC Board Financial and Audit Committee, and external auditors
Expert records (including evaluation and violation records)	Limited to the Director of the IQA Office, expert management personnel, and investigation team members in appeal investigations (case-related parts only)

(2) All record access operations shall generate system audit logs, recording the visitor's identity, access time, accessed records and access type (view, download, print, etc.). The retention period of audit logs shall not be shorter than that of the accessed records.

(3) Dedicated record management personnel shall conduct random inspections of access logs on a quarterly basis and report abnormal access to the Director of the IQA Office in a timely manner.

Article 14 Data Transmission and Sharing

(1) Electronic records shall be transmitted via encrypted channels. Records containing sensitive information shall not be transmitted via unencrypted emails or public instant communication tools.

(2) External sharing of records beyond the IQA system shall be approved by the Director of the IQA Office and accompanied by a signed data sharing agreement. The minimum scope principle shall be applied for record sharing — only necessary parts of records shall be provided instead of complete case files.

(3) Cross-border transmission of records involving personal data shall comply with the cross-border data transmission provisions of the *IAPUC Digital Security and Privacy Regulations*.

Chapter V Record Destruction

Article 15 Initiation of Destruction

(1) For records whose retention periods have expired and no extension circumstances specified in Article 9 of these Rules apply, dedicated record management personnel shall compile a*Record Destruction List* and initiate the destruction procedure.

(2) When compiling the destruction list, dedicated record management personnel shall verify item by item that each record:

1. Has indeed expired retention period;

2. Is not involved in ongoing appeals, complaints, investigations or litigation;

3. Has no additional retention obligations stipulated by laws or contracts.

Article 16 Destruction Approval

(1) The *Record Destruction List* shall be approved level by level by the following personnel:

1. Confirmation and signature by dedicated record management personnel;

2. Review and verification by the Director of the IQA Office;

3. Filing and consent by the Chair of the Accreditation Decision Committee for the destruction of institutional accreditation records and review & decision records.

(2) Approvers who have objections to record destruction decisions may suspend destruction and conduct re-verification. Relevant records shall not be destroyed during the re-verification period.

Article 17 Destruction Methods and Records

(1) Electronic Record Destruction

1. Adopt irreversible secure erasure methods (such as multiple overwriting, encryption key destruction) or physical destruction of storage media;

2. Corresponding data in backup systems shall be destroyed synchronously without omission;

3. Cloud-stored records shall be completely deleted from cloud servers and all redundant nodes.

(2) Paper Record Destruction

1. Adopt cross-cut shredders (with shredded particle area no larger than 320mm²) or professional confidential destruction services;

2. If entrusted to third-party institutions for destruction, a confidential destruction agreement shall be signed, and the destruction process shall be supervised by on-site IQA staff or verified via official signed destruction certificates issued by third parties.

(3) Within 30 days after completion of destruction, dedicated record management personnel shall compile a *Record Destruction Log*, specifying:

1. Name, category and file number/batch number of destroyed records;

2. Quantity and carrier form of destroyed records;

3. Destruction date and method;

4. Signatures of approvers and executors.

(4) The *Record Destruction Log* shall be permanently retained as an official record.

Chapter VI Accredited Institutions' Record Obligations

Article 18 Institutional Internal Accreditation Record

Retention

(1) Accredited institutions shall formulate and implement internal accreditation record retention systems in accordance with the retention period standards specified in Chapter III of these Rules.

(2) Institutional quality representatives shall be responsible for the integrity and security of internal institutional accreditation records. Records shall be retained in an organized and retrievable manner and provided promptly upon IQA's request for inspection.

Article 19 Record Disposal After Institutional Closure or Accreditation Termination

(1) If an institution ceases to hold accreditation qualifications due to closure, merger, accreditation revocation or other reasons, it shall still bear the obligation to retain records generated during the accreditation period, and the retention obligations shall not terminate due to accreditation cessation.

(2) Before institutional closure or dissolution, the institution shall submit a written report on its accreditation record disposal plan to the IQA Office. The IQA Office has the right to require the institution to transfer designated records to IQA or a designated third-party record management institution, with all relevant expenses borne by the institution.

(3) If an institution entrusts a third party with record custody, it shall sign a custody agreement containing confidentiality clauses and submit a copy of the agreement to the IQA Office for filing.

Chapter VII Supervision and Compliance

Article 20 Internal Audit

(1) The Director of the IQA Office shall conduct an annual internal inspection of record management, covering at least the following contents:

1. Completeness and timeliness of record filing;

2. Compliance of record retention periods;

3. Compliance of access authority and access logs;

4. Compliance of destruction procedures;

5. Verification of backup recoverability.

(2) Internal inspection reports shall be filed with the Director of the IQA Office and the Accreditation Decision Committee. Rectification plans shall be formulated and implemented within 60 days for identified problems.

Article 21 Response to Record Security Incidents

(1) In the event of record loss, unauthorized access, information leakage, damage or other security incidents, the IQA Office shall initiate emergency response within 24 hours upon discovery.

(2) Incident response procedures shall be implemented in accordance with Article 17 of the *IAPUC Digital Security and Privacy Regulations*. For incidents involving institutional submitted records, the IQA Office shall notify the affected institutions within 72 hours after incident confirmation.

Article 22 Violation Disposal

(1) IQA internal staff who violate the provisions of these Rules in record management shall be subject to disciplinary sanctions including warning, suspension of authority or other corresponding penalties based on the severity of violations.

(2) Accredited institutions that violate cooperation obligations in record management, intentionally omit submitted records or destroy records that should be retained shall be deemed in breach of accreditation compliance obligations. The IQA Office may include such acts as negative factors in accreditation supervision, and record them as negative findings in annual reviews or re-evaluations for serious violations.

Chapter VIII Supplementary Provisions

Article 23 Relationship with Other Normative Documents

These Rules constitute a unified IAPUC-IQA normative system together with the following documents:

Document	**Relationship with These Rules**
IAPUC Digital Security and Privacy Regulations	These Rules serve as operational elaborations in the field of record management, with the Regulations as the superior basis for data security, access control and cross-border transmission
IAPUC-IQA Accreditation Procedure Specifications	These Rules specify operational norms for the filing, retention and destruction of documents generated at all stages of the accreditation procedures
IQA Accreditation Appeals, Complaints and Dispute Resolution Management Measures	The case filing retention period and confidentiality management requirements stipulated in the Measures are specifically implemented and regulated by these Rules

IQA Institutional Quality Representative Management Measures	Institutional internal record management obligations are implemented and guaranteed through the duties of quality representatives

Article 24 Term Definitions

Term	Definition
Accreditation Records	Records existing in any carrier form that are generated or received in IQA accreditation activities and possess evidentiary value and business reference value
Retention Period	The minimum retention duration of records starting from the commencement date, during which records shall not be destroyed
Secure Erasure	A deletion method that adopts technical means to render electronic data unrecoverable, which is different from ordinary deletion
Audit Log	Tamper-proof automatic records of operations including record access, modification and destruction

Article 25 Interpretation and Revision of the Rules

(1) These Rules shall be interpreted by the IAPUC Quality Accreditation Committee.

(2) Any revision of these Rules shall be subject to the approval of the IAPUC Council. Adjustments to record retention periods shall not apply retroactively to records whose retention periods have expired prior to the entry into force of the revised version.

Article 26 Entry into Force and Transitional Provisions

These Rules shall come into force officially upon approval by the IAPUC Council. All records stored in the repository at the time of entry into force shall be governed by the following transitional rules:

(1) For records with expired retention periods, the destruction approval procedures shall be completed within 180 days after the entry into force of these Rules;

(2) For records with unexpired retention periods, the records shall be retained continuously in accordance with the retention period provisions stipulated in these Rules.

Appendix: Record Destruction Approval and Record

Form

The form shall include the following mandatory items:

1. Record Category and Name

2. Record Number / Batch Number

3. Expiry Date of Retention Period

4. Existence of Retention Extension Circumstances (Yes/No)

5. Destruction Method

6. Approval Column (Record Management Specialist, IQA Office Director, ADC Chair for Filing)

7. Execution Record (Destruction Date, Executor, Supervisor, Post-destruction Confirmation)

Document Approval

Role	Name / Position	Date
Drafting	IAPUC Quality Accreditation Committee Archive Management Standards Working Group	May 2026
Review	IAPUC Quality Accreditation Committee	To be confirmed
Approval	IAPUC Council	To be confirmed

Copyright Statement