

Document 3: IQA Certification Archives and Data Retention Management Detailed Rules

: IAPUC/IQA/REC-2026-001

: 1.0

: To be officially released

: IAPUC Quality Certification Committee

: The IQA Office, peer review experts, members of the certification decision-making body, members of the appeal and arbitration committee, and all private higher education institutions that have obtained or are applying for IQA certification.

Preface

Certification archives serve as the institutional memory of the credibility of the IAPUC-IQA certification system. Each self-evaluation report, each review record, and each decision-making process not only records the quality pursuit trajectory of certified institutions, but also forms the cornerstone of the transparency and traceability of the certification system. The massive volume of data and archives generated in certification activities are not only public assets that guarantee the right to know of stakeholders, but also bear the legitimate rights and interests and privacy expectations of institutions, teachers, students and review experts. Balancing and , and ensuring the integrity and security of archives while respecting the rights of data subjects, constitute the core issues that must be addressed in certification archive management.

These Detailed Rules are formulated to establish a full life-cycle management specification for all archives and data generated in IQA certification activities, covering generation, archiving, preservation, utilization and final destruction. Adopting the design principle of , these Rules are closely aligned with the and the , jointly building an information governance defense line for the certification system.

Chapter One General Provisions

Article 1 Purposes and Basis

These Detailed Rules are formulated for the following purposes:

- (1) To define the scope, types and ownership of IQA certification archives and data;
- (2) To establish a classified retention period system based on archive sensitivity and

- business value, ensuring compliant retention and scheduled cleanup of archives;
- (3) To formulate security management standards for archive storage, access, transmission and destruction;
- (4) To balance archive utilization and confidentiality protection, and safeguard the legitimate rights and interests of data subjects;
- (5) To clarify the cooperative obligations of certified institutions in certification archive management.

These Detailed Rules are formulated in accordance with:

- The provisions on data life cycle management and technical security measures stipulated in the ;
- The provisions on document submission and confidentiality obligations at all stages of certification specified in the ;
- The archive management requirements for case handling stipulated in the ;
- The General Principles for Archival Management issued by the International Council on Archives (ICA);
- ISO 15489-1:2016 Information and Documentation — Records Management Standards.

Article 2 Scope of Application

These Detailed Rules shall apply to:

- (1) All archives and data generated and received by the IQA Office in certification management activities;
- (2) All archives and data generated and accessed by peer review experts, members of the certification decision committee, and members of the appeal and arbitration committee in certification activities;
- (3) All certification-related documents submitted by certified institutions and derived review and decision documents;
- (4) Official archives related to IQA certification retained by certified institutions themselves.

Article 3 Basic Principles

The management of IQA certification archives shall implement the following basic principles:

Principle	Core Connotation
Integrity	A complete archive chain shall be formed throughout the entire certification process to ensure traceability

	and auditability of decision-making procedures.
Security	The storage, transmission and access of archives shall adopt security protection measures matching the sensitivity level of archives.
Minimum Retention	The retention period of archives shall not exceed the time necessary for business operation and legal obligations, and expired archives shall be destroyed in accordance with regulations.
Traceability	All operations including archive access, authorized modification and destruction shall be recorded to form an immutable audit log.
Clear Rights and Obligations	The rights and responsibilities of archive generators, managers, users and destruction approvers shall be clearly defined with each party performing its own duties.

Chapter Two Archive Classification and Scope

Article 4 Archive Classification

Based on business sources and information attributes, IQA certification archives are divided into the following five categories:

(1) Institutional Certification Archives

Archives submitted by certified institutions and generated by IQA in institutional certification activities, including:

Certification application documents and qualification review materials;

Self-evaluation reports and all supporting evidence materials;

Annual quality monitoring reports and mid-term self-evaluation briefings;

Major change reports and relevant processing records;

Quality representative appointment letters, change records and communication archives;

Certification fee payment and financial transaction records;

Certificate issuance and certification status publicity records;

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

(2) Review and Decision-Making Archives

Archives generated in the certification review and decision-making process, including:

Peer review team formation and appointment records;

Conflict of interest statements and confidentiality commitment letters of review experts;

Desk review working papers and issue lists;

On-site inspection records — summaries of forums and interviews, facility inspection records, evidence verification records (excluding original notes involving personal privacy of review experts, based on official summaries sorted and submitted by experts in accordance with team resolutions);

Peer review reports and opinions of review team members (including minority opinions);

Institutional response opinions to review reports;

Certification decision committee meeting minutes and voting records;

Certification decision notices.

(3) Appeal, Complaint and Dispute Resolution Archives

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

Appeal petitions, complaint petitions and dispute mediation applications;

Case filing review and investigation records;

Working records and reports of review and investigation teams;

Hearing records (if applicable);

Rulings, handling decisions and settlement agreements;

Whistleblower protection records.

(4) Expert and Personnel Management Archives

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

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

Expert training and assessment records;

Expert evaluation and grade promotion records;

Expert violation investigation and disposal records;

Expert exit records;

Performance and compliance records of IQA Office staff;

Confidentiality commitment letter signing records.

(5) Financial and Administrative Archives

Archives generated in IQA certification financial and administrative management, including:

Annual budget and final account documents;

Audit reports and management suggestion responses;

Fee standard formulation and adjustment records;

Revenue and expenditure vouchers and accounting books;

Contracts and agreement documents.

Article 5 Archive Carriers

The carriers of IQA certification archives include:

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

(2) Paper Archives: Original or copied archives in paper form;

(3) Hybrid Archives: Archives of the same business matter existing in both electronic and paper carriers. Associated indexes shall be established in the archive management system to ensure mutual queryability of dual-track archives.

Article 6 Archiving Scope and Responsible Persons

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

(2) After the completion of review tasks, the review team leader shall sort and archive the review working papers (based on the officially submitted archived version), official on-site inspection summaries and review reports to the IQA Office within 30 days after submission.

(3) The meeting minutes and voting records of the certification decision committee shall be archived by the committee secretary within 15 days after the completion of decision-making.

(4) The case files of the appeal and arbitration committee shall be archived by the committee secretary within 30 days after case closure.

(5) Financial archives shall be archived within 60 days after the completion of annual audit by fiscal year.

(6) The IQA Office shall appoint dedicated archive management personnel responsible for the daily management of archive receipt, classification, cataloging,

preservation and destruction.

Chapter Three Retention Periods

Article 7 Principles for Setting Retention Periods

Archive retention periods are comprehensively determined based on the following factors:

- (1) The business reference value of archives for current and future certification activities;
- (2) The retrospective needs for potential appeals, complaints or legal disputes;
- (3) Statutory retention requirements for financial and legal compliance;
- (4) The sensitivity of archive information — highly sensitive personal data shall be retained for the shortest possible period on the premise of meeting business and legal requirements.

Article 8 Retention Period Table

Archive Category	Archive Content	Retention Period	Calculation Start Date
Permanent Retention	Final certification decision records (including voting results) of the Certification Decision Committee	Permanent	Effective date of the decision
Permanent Retention	Official certificate issuance records and certification status history	Permanent	Effective date of initial certification
Permanent Retention	Historical versions of certification standards, manuals and major normative documents	Permanent	Effective date of the version
Long-term	Institutional self-	15 years after the	Expiration date of

Retention	evaluation reports and supporting materials (certified institutions)	expiration of the certification validity period	the certification validity period
Long-term Retention	Peer review reports and institutional responses	15 years after the expiration of the certification validity period	Expiration date of the certification validity period
Long-term Retention	Appeal and arbitration case rulings	15 years after case closure	Case closure date
Medium-term Retention	Institutional self-evaluation reports and supporting materials (uncertified institutions)	10 years after the effective date of the non-certification decision	Effective date of the decision
Medium-term Retention	Annual quality monitoring reports	10 years after submission	Submission date
Medium-term Retention	Major change reports and processing records	10 years after submission	Submission date
Medium-term Retention	Complete appeal and complaint case files (excluding rulings)	10 years after case closure	Case closure date
Medium-term Retention	Review expert archives (including database entry, evaluation, violation disposal and exit records)	10 years after expert exit	Expert exit date
Medium-term Retention	Financial archives – budgets, final accounts and	10 years after audit completion	Issuance date of the audit report

	audit reports		
Standard Retention	Qualification review materials (including informal communication records)	5 years after decision	Effective date of the decision
Standard Retention	Desk review working papers and issue lists	5 years after review completion	Submission date of the review report
Standard Retention	Conflict of interest statements and confidentiality commitment letters of review experts	5 years after completion of review tasks	Submission date of the review report
Standard Retention	On-site inspection forum summaries and evidence verification records	5 years after review completion	Submission date of the review report
Standard Retention	Financial archives – revenue and expenditure vouchers, accounting vouchers	7 years after audit completion	Issuance date of the audit report
Standard Retention	Certification fee payment records	7 years after payment	Payment date
Short-term Retention	General administrative correspondence and informal communication records	3 years after communication conclusion	Correspondence conclusion date
Short-term Retention	Drafts, temporary notes and working	1 year after completion of	Completion date of the matters

	documents not formally included in case files	relevant matters	
--	---	------------------	--

Article 9 Extension of Retention Periods

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

Archives involved in ongoing appeals, complaints or legal proceedings shall be retained for an additional 5 years after the final adjudication of the case and exhaustion of all remedy channels;

Archives involved in ongoing investigations or audits shall be retained for an additional 5 years after the conclusion of the investigation or audit;

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

(2) Archive management personnel shall mark extended retention archives in the archive management system, specifying the extension reasons and new retention period.

Article 10 Institutional Self-Archive Retention

Certified institutions shall formulate and implement internal certification archive retention systems in accordance with the retention period standards stipulated herein. During on-site certification inspections or subsequent reviews, institutions shall provide complete certification archives within the retention period. If an institution is unable to continue retaining archives due to relocation, merger, closure or other reasons, it shall notify the IQA Office 60 days in advance to negotiate archive handover or disposal solutions.

Chapter Four Storage and Security Management

Article 11 Electronic Archive Storage

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

(2) Electronic archives shall be protected by the following technical measures:

Encrypted Storage: Archives containing sensitive personal data shall be encrypted at the storage layer;

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

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

Tamper Resistance: Officially archived electronic archives shall be set to read-only status. Any authorized modification shall retain complete modification logs and pre- and post-modification version comparisons;

Format Management: Open standard or long-term readable file formats shall be prioritized for archive storage to avoid unreadable archives caused by obsolete software.

(3) The integrity of electronic archive storage media shall be verified regularly, and data migration shall be carried out in a timely manner for degraded media.

Article 12 Paper Archive Storage

(1) Paper archives shall be stored in dedicated archives or filing cabinets designated by the IQA Office, with environments meeting the basic requirements of fire prevention, moisture proofing, insect prevention and light prevention.

(2) Highly sensitive paper archives (e.g. documents containing large-scale student personal data) shall be locked or sealed for custody, and access shall be subject to approval by archive management personnel.

(3) Paper archives with long-term retention value are encouraged to be digitally scanned and their digital copies shall be managed in accordance with the same standards as electronic archives. However, scanned copies shall not automatically replace the retention obligation of original paper documents — originals shall still be retained in accordance with the periods stipulated herein, unless the retention of only digital copies is approved by the Director of the IQA Office.

Article 13 Access Control

(1) The access rights of IQA certification archives shall be managed based on the principle:

Archive Category	Access Rights
Institutional certification application and self-evaluation materials	Authorized staff of the IQA Office, review team members of the case, ADC members (during decision review), appeal review team members (during appeal acceptance)
Review reports and decision records	In addition to the above personnel, authorized academic researchers engaged in certification quality research may access the archives after desensitization upon approval by the Director of the IQA Office

Institutional self-owned archives	Institutions have the right to access all materials submitted by themselves and review reports related to the institution within the retention period
Appeal and complaint case files	Limited to members of the appeal and arbitration committee, investigation team members and personnel authorized by the Director of the IQA Office
Financial archives	Limited to IQA finance staff, treasurers, members of the IAPUC Board Financial and Audit Committee, and external auditors
Expert archives (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 archive access operations shall generate system audit logs, recording the visitor's identity, access time, accessed archive objects and access types (view, download, print, etc.). The retention period of audit logs shall not be shorter than that of the accessed archives.

(3) Archive 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 archive transmission shall adopt encrypted channels. Archives containing sensitive information shall not be transmitted via unencrypted emails or public instant communication tools.

(2) External sharing of archives outside the IQA system shall be approved by the Director of the IQA Office and a data sharing agreement shall be signed. The minimum scope principle shall apply to archive sharing — only necessary parts shall be provided instead of the entire case file.

(3) Cross-border transmission of archives involving personal data shall comply with the cross-border data transmission provisions of the .

Chapter Five Destruction

Article 15 Initiation of Destruction

(1) For archives whose retention periods have expired and are not subject to the

extension circumstances specified in Article 9 herein, archive management personnel shall compile the to initiate the destruction procedure.

(2) When compiling the destruction list, archive management personnel shall verify item by item whether the archives:

Have indeed expired retention periods;

Are not involved in ongoing appeals, complaints, investigations or litigation;

Have no additional retention obligations stipulated by laws or contracts.

Article 16 Destruction Approval

(1) The shall be approved level by level by the following personnel:

Confirmed and signed by archive management personnel;

Reviewed by the Director of the IQA Office;

The destruction of institutional certification archives and review decision-making archives shall be filed and consented by the Chair of the IQA Quality Certification Decision Committee.

(2) Approvers who have objections to the archive destruction decision may require deferred destruction and review. Relevant archives shall not be destroyed during the review period.

Article 17 Destruction Methods and Records

(1) Electronic archive destruction:

Adopt non-recoverable secure erasure methods (such as multiple overwriting, encryption key destruction) or physical destruction of storage media;

Corresponding data in the backup system shall be destroyed synchronously without omission;

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

(2) Paper archive destruction:

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

Where third-party destruction is entrusted, a confidential destruction agreement shall be signed, and the destruction process shall be supervised by IQA staff or a signed and sealed destruction certificate shall be issued by the third party.

(3) Within 30 days after the completion of destruction, archive management personnel shall compile the , specifying:

Name, category and archive number of destroyed archives;

Quantity and carrier type of destroyed archives;

Destruction date and method;

Signatures of approvers and executors.

(4) The itself shall be permanently retained as an archive.

Chapter Six Archive Obligations of Certified Institutions

Article 18 Institutional Internal Certification Archive Retention

(1) Certified institutions shall formulate and implement internal certification archive retention systems in accordance with the retention period standards in Chapter Three herein.

(2) The institutional quality representative shall be responsible for the integrity and security of internal institutional certification archives. Archives shall be retained in an orderly and retrievable manner to ensure timely provision when the IQA requests inspection.

Article 19 Archive Disposal After Institutional Closure or Certification Termination

(1) If a certified institution ceases to hold certification qualifications due to closure, merger, certification revocation or other reasons, it shall still bear the retention obligation for archives generated during the certification period, and the retention obligation shall not terminate due to certification termination.

(2) Before institutional closure or dissolution, the institution shall submit a written report on the certification archive disposal plan to the IQA Office. The IQA Office has the right to require the institution to hand over designated archives to IQA or a designated third-party archive management institution, with relevant expenses borne by the institution.

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

Chapter Seven Supervision and Compliance

Article 20 Internal Audit

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

- Completeness and timeliness of archiving;
- Compliance of retention periods;
- Compliance of access rights and access logs;
- Compliance of destruction procedures;
- Backup recoverability verification results.

(2) The internal inspection report shall be filed with the Director of the IQA Office and the Certification Decision Committee. Problems identified shall be rectified within 60 days by formulating and implementing rectification plans.

Article 21 Archive Security Incident Response

- (1) In the event of archive loss, unauthorized access, leakage, damage or other security incidents, the IQA Office shall initiate an emergency response within 24 hours upon discovery.
- (2) The incident response procedure shall be implemented in accordance with Article 17 of the . For incidents involving archives submitted by certified institutions, the IQA Office shall notify the affected institutions within 72 hours after confirming the incident.

Article 22 Violation Disposal

- (1) IQA internal staff who violate these Rules in archive management shall be given warnings, suspension of authority or other corresponding disciplinary sanctions according to the severity of the circumstances.
- (2) Certified institutions that violate cooperation obligations in archive retention, or intentionally omit or destroy archives that should be retained in archive submission, shall be deemed to have violated certification compliance obligations. The IQA Office may include such acts as negative factors in certification supervision, and may record them as negative findings in annual reviews or re-evaluations for serious circumstances.

Chapter Eight Supplementary Provisions

Article 23 Relationship with Other Normative Documents

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

Document	Relationship with These Rules
	These Rules are the operational expansion in the

	field of archive management, with the Regulations as the superior basis for data security, access control and cross-border transmission
	These Rules provide operational specifications for archiving, retention and destruction of documents generated at all process stages
	The file archiving retention period and confidentiality management requirements stipulated in the Measures are specifically regulated and implemented by these Rules
	The internal archive obligations of certified institutions are implemented and guaranteed through the duties of quality representatives

Article 24 Term Definitions

Term	Definition
Certification Archives	Records generated or received in IQA certification activities in any carrier form with evidential value and business reference value
Retention Period	The minimum time length for which archives must be retained from the calculation start date, and shall not be destroyed before expiration
Secure Erasure	A technical method to delete electronic data irrecoverably, different from ordinary deletion
Audit Log	Immutable automatic records of archive access, modification and destruction operations

Article 25 Interpretation and Revision of Rules

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

(2) The revision of these Rules shall be approved by the IAPUC Council.

Adjustments to retention periods shall not apply retroactively to archives whose retention periods have expired before the revision takes effect.

Article 26 Entry into Force and Transitional Provisions

These Rules shall come into force officially upon approval by the IAPUC Council. For existing archives upon the entry into force of these Rules, the following transition rules shall apply:

(1) Archives with expired retention periods shall complete the destruction approval procedure within 180 days after the entry into force of these Rules;

(2) Archives with unexpired retention periods shall be retained continuously in accordance with the retention periods stipulated herein.

Appendix: Archive Destruction Approval and Record Form

The form shall include the following contents:

Archive Category and Name

Archive No. / Batch No.

Expiration Date of Retention Period

Whether there is an extension circumstance (Yes / No)

Destruction Method

Approval Column (Archive Management Personnel, IQA Office Director, ADC Chair Filing)

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

Document Approval

Role	Name / Position	Date
Compiled by	IAPUC Quality Certification Committee Archive Management Standard Working Group	May 2026
Reviewed by	IAPUC Quality Certification Committee	Pending
Approved by	IAPUC Council	Pending

Copyright Statement

The intellectual property rights of this document and the IQA Certification Archives

and Data Retention Management Detailed Rules contained herein belong to the International Association of Private Universities and Colleges (IAPUC). Without written authorization from IAPUC, no institution or individual may copy, modify or use this document for commercial purposes. Certified institutions may freely use this document for internal institutional system construction purposes.