Data Retention Policy

|  |  |
| --- | --- |
| Policy Area | IT Policy Library |
| Approved Date | December 31, 20XX |
| Approved By | Policy Committee |
| Effective Date | January 1, 20XX |
| Current Version | 1.0 |

# I. Overview

ABC Company must balance our legal obligations and need to retain information for business purposes against the cost of storing and securing such information.

# II. Purpose

This policy helps manage risks related to legal and compliance requirements and our ability to continue business operations.

# III. Scope

This policy applies to all Staff that have access or and data retention responsibilities for ABC Company’s Information Resources.

# IV. Policy

A. Responsibilities

ABC Company’s Legal Department shall establish enterprise-wide retention procedures for the organization. In establishing ABC Company’s retention procedures, the Legal Department shall consider legal and compliance requirements, litigation needs, business processes, privacy concerns, and the cost of retaining information.

The Legal Department is responsible for preparing and maintaining a comprehensive data retention, archiving, and destruction schedule (Retention Schedule). The Retention Schedule will consider active and inactive electronic information including data held in servers, databases, storage arrays, backup media, important workstations, e-mail, log files, video cameras, and other types of electronic storage devices.

When establishing retention periods, the Legal Department will perform the following steps:

* Determine applicable legal or compliance requirements.
* Determine, with the help of ABC Company Departments, the collection, storage, archiving, and use of electronically stored data.
* Identify other internal or external Departments or business entities that collect, store, archive, or use electronically stored information.
* Establish retention periods for electronically stored information based on information obtained in the prior steps.

Each ABC Company department will develop procedures and documentation that implement and maintain the retention requirements as outlined in the Retention Schedule. The specific procedures implemented by each Department will specify the retention time, archival rules, data formats, and the permissible means of storage, access, and encryption (if any).

B. Retention Requirements

The Chief Security Officer (CSO) shall:

* Implement data retention and disposal guidelines that limiting data storage amount and retention time to that which is required for legal, regulatory, and business requirements.
* Ensure quarterly automatic or manual processes exist for the secure deletion of data when no longer needed.
* Establish specific retention requirements for sensitive data.

Different types of data require different retention periods. In addition to describing how long various types of information must be maintained, department retention procedures must specify:

* Steps used to archive the information.
* The appropriate destruction of electronically stored information after the identified retention period. Such steps shall adhere to the requirements outlined in the Disposal Policy.
* Procedures for handling electronically stored information when under litigation.

Each department may have unique data retention requirements that must be communicated to the Legal Department. Such requirements may include contractual obligations with customers or business contacts or data retention requirements to maintain business operations. In some instances, departments may need to retain electronically stored information for a historical archive.

To meet regulatory and organizational requirements, the Legal Department:

* Will identify retention periods for log files and audit trails.
* May choose to alter e-mail retention requirements specified in the E-mail Policy.

During the appropriate retention period, archived data must be retrievable.

* As new software and/or hardware is implemented, the IT Department shall ensure that new systems can read legacy data. This may require old data be converted to new formats.
* Data that is encrypted must be retrievable. The IT Department shall implement key management procedures that ensure encrypted data can be decrypted when needed.

C. Retention Resources

When establishing retention periods, the Legal Department may rely on one or more of the following legislative requirements.

Code of Federal Regulations - organizations must retain compliance evidence for not less than 2 years in a form that is capable of accurately retaining and reproducing information. If the organization is being investigated, it must retain the records pertaining to the action until final disposition, unless disposal is allowed by court order. [ 229.21(g), 12 CFR Part 229 Availability of Funds and Collection (Check Clearing for the 21st Century)]

Energy - retain all records and the supporting technical documentation required to satisfy this section's requirements until the license for which the records were developed has been terminated by the Nuclear Regulatory Commission. Superseded portions of records must be retained for at least 3 years after being superseded, unless the Commission has specified otherwise. [ 73.54(h), 10 CFR Part 73.54, Protection of digital computer and communication systems and networks]

Healthcare

* Records shall be kept for a time period equal to the design and expected life of the device, but not less than 2 years from the commercial distribution release date. [ 820.180(b), 21 CFR Part 820, Subchapter H - Medical Devices, Part 820 Quality System Regulation]
* Required documentation shall be kept for 6 years from the creation date or the date it was last in effect, whichever is later. [ 164.316(b)(2)(i), 45 CFR Parts 160, 162, and 164, Health Insurance Reform: Security Standards, Final Rule]
* Eligible hospitals, eligible professionals (EPs), and critical access hospitals (CAHs) must keep documentation that supports the demonstration of meaningful use for 6 years. [ 495.8(c)(2), 422.504(d), 495.8(c)(2), 42 CFR Parts 412, 413, 422 et al., Medicare and Medicaid Programs; Electronic Health Record Incentive Program, Final Rule]
* Documentation required by 164.530(j)(1) must be retained for 6 years from the creation date or the date it was last in effect, whichever is later. [ 164.530(j)(2), 45 CFR Parts 160 and 164, Standards for Privacy of Individually Identifiable Health Information, Final Rule]
* The Records Officer must ensure signed forms and related documentation, for personnel departures, are kept in a centralized file for at least 10 years in the Records Management or Personnel office. [Department of Health and Human Services Records Management Procedures Manual, Version 1.0 Final Draft]

National Association of Securities Dealers - keep all such documents for a period of not less than 5 years, the first 2 years in an easily accessible place, subject to the destruction and disposition provisions of Rule 17a–6. [ 240.17a-6(b), 17 CFR Part 240.17a-1, Recordkeeping rule for securities exchanges]

Payment Card Industry (PCI)

* The organization must ensure audit trails are retained for at least 1 year and must have the last 3 months available for immediate analysis (i.e. on-line, archived, or restorable from backup). [ 10.7, Payment Card Industry (PCI) Data Security Standard, Requirements and Security Assessment Procedures ]
* Examine security policies and procedures and verify that they include audit log retention policies and require audit log retention for at least 1 year with the most recent 3 months available. [ 10.7.a Testing Procedures, Payment Card Industry (PCI) Data Security Standard, Requirements and Security Assessment Procedures ]
* Keep cardholder data storage to a minimum by implementing data retention and disposal policies, procedures and processes that include at least the following for all cardholder data storage: Limit data storage amount and retention time to that which is required for legal, regulatory, and/or business requirements, specific retention requirements for cardholder data, processes for secure deletion of data when no longer needed, and a quarterly process for identifying and securely deleting stored cardholder data that exceeds defined retention. [ 3.1 Protect Stored Cardholder Data, Payment Card Industry (PCI) Data Security Standard, Requirements and Security Assessment Procedures ]

Sarbanes Oxley - The organization must prepare and maintain audit work papers and other information for not less than 7 years. [ 103(a)(2)(A)(i), 1520(a)(2), The Sarbanes-Oxley Act of 2002 (SOX)]

Tax - Records of the requests by or to the organization for Federal Tax Information must be maintained for 5 years. [ 5.01(1), IRS Revenue Procedure: Record retention: automatic data processing, 98-25]

U.S. Federal Security - All required records must be kept for a period of 5 years. [ 762.6(a), US Export Administration Regulations Database]

Various State Laws - When a breach investigation concludes that the breach has not and will not likely result in harm to any individuals, the organization must document the non-notification requirement in writing and maintain the documentation for 5 years.

[ 45.48.010(c), Alaska Personal Information Protection Act, Chapter 48]

[ 817.5681(10), Florida Statute 817.5681 Breach of security concerning confidential personal information in third-party possession]

[ 715C.2.6, Iowa Code Annotated 715C Personal Information Security Breach Protection]

[ 14-3504(b)(4), Maryland Code of Commercial Law Subtitle 35. Maryland Personal Information Protection Act 14-3501 thru 14-3508] (3 years)

[ 407.1500.2(5), Missouri Revised Statutes Chapter 407 Merchandising Practices 407.1500]

[ 56:8-163.a, New Jersey Permanent Statutes Title 56 Security of Personal Information]

# V. Enforcement

Any Staff member found to have violated this policy may be subject to disciplinary action, up to and including termination.

# VI. Distribution

This policy is to be distributed to all ABC Company Staff.

**Policy History**

|  |  |  |  |
| --- | --- | --- | --- |
| Version | Date | Description | Approved By |
| 1.0 | 1/1/20XX | Initial policy release |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

**References:**

COBIT EDM01.01, EDM03.02, APO01.11, APO12.07, APO14.01-02, APO14.07, APO14.10

GDPR Article 5

HIPAA 164.316(b)(2)(i)

ISO 27001 A.8.2, A.8.3.2

NIST SP 800-37 3.2, 3.7

NIST SP 800-53 AC-16, AT-4, AU-11, MP-6, SA-19(3), SI-12

NIST Cybersecurity Framework ID.AM-2, ID.AM-4, ID.GV-3, PR.IP-6

PCI 3.1, 10.7