**Record Retention and Data Destruction Policy**

**Organization: The Xander Protocol**

**Policy Owner: Chief Compliance & Records Officer (CCRO)**

**Approval Date: 10/22/2025**

**Version: 1.0**

**Review Cycle: Annual**

**Classification: Internal / Confidential**

**Table of Contents**

**1. Executive Summary**

**2. Purpose**

**3. Scope**

**4. Regulatory & Framework Alignment**

**5. Key Definitions**

**6. Governance Principles**

**7. Record Retention Requirements**

**8. Data Destruction and Erasure Procedures**

**9. Access Control and Responsibilities**

**10. Software, Systems, and Updates**

**11. Training and Awareness**

**12. Monitoring and Biannual Review**

**13. Incident Response**

**14. Continuous Improvement and Enforcement**

**1. Executive Summary**

This policy establishes corporate-wide standards for record retention, data lifecycle management, and secure destruction of information. It ensures that records are maintained only as long as necessary, protects sensitive information, aligns with regulatory requirements, and reduces operational and legal risk.

**2. Purpose**

• Define requirements for retention, maintenance, and destruction of corporate records.

• Protect confidential and sensitive data from unauthorized access or misuse.

• Ensure compliance with regulatory frameworks and internal governance standards.

• Promote a culture of accountability and operational efficiency across all staff.

**3. Scope**

• Applies to all employees, contractors, and temporary staff.

• Covers operational staff, IT teams, management, and executive personnel.

• Includes all corporate records, digital and physical, across business units.

• Encompasses training, document creation, storage, access, maintenance, and destruction.

**4. Regulatory & Framework Alignment**

• ISO 27001: Information security and record management controls.

• NIST CSF: Data protection and operational risk management.

• GDPR / CCPA: Privacy and personal data retention requirements.

• SOX / GLBA / HIPAA: Industry-specific retention and audit compliance where applicable.

• Internal Policies: Alignment with corporate governance and operational procedures.

**5. Key Definitions**

• Record: Any document, electronic file, or physical material created or received in the course of business.

• Retention Period: The length of time a record is maintained before destruction.

• Data Erasure: Secure deletion of digital records, ensuring recovery is not possible.

• Data Destruction: Physical destruction of materials such as paper files, CDs, or storage devices.

• Critical Records: Records that must be preserved beyond standard retention due to legal, financial, or operational obligations.

**6. Governance Principles**

• Maintain only relevant, necessary records.

• Apply least privilege to access and management of records.

• Align retention and destruction practices with regulatory and legal requirements.

• Document all retention schedules, destruction actions, and responsibilities.

• Promote awareness and compliance across all staff levels.

**7. Record Retention Requirements**

• Categorize records by type (e.g., financial, operational, HR, legal, technical).

• Define retention periods for each category, with timelines clearly documented.

• Critical or regulatory-required records may have extended retention schedules.

• Notify responsible parties prior to scheduled destruction for review or extension.

• Avoid indefinite retention unless legally or operationally required.

**8. Data Destruction and Erasure Procedures**

• Apply secure erasure techniques for digital records, including overwriting, hashing, or degaussing.

• Destroy physical records via shredding, incineration, or approved secure destruction methods.

• Double-check for duplicate copies or backups before destruction.

• Maintain documentation of destruction events including date, responsible personnel, and type of data destroyed.

• Restrict destruction of sensitive or critical records until compliance confirmation.

**9. Access Control and Responsibilities**

• Only authorized personnel may manage, maintain, or destroy records.

• Supervisors and record owners ensure proper adherence to retention and destruction timelines.

• IT and security teams manage access to electronic storage, backups, and archival systems.

• Employees are responsible for understanding and following retention schedules relevant to their role.

**10. Software, Systems, and Updates**

• Utilize corporate-approved software and systems for record management.

• Ensure systems are updated to prevent data loss, corruption, or unauthorized access.

• Maintain secure backups to allow recovery of records within retention periods.

• Review system capabilities annually to align with retention and destruction policy.

**11. Training and Awareness**

• Mandatory onboarding training for all employees on retention and destruction practices.

• Biannual refreshers and reminders to ensure compliance awareness.

• Include practical guidance on recognizing record types, retention periods, and destruction procedures.

• Encourage reporting of potential violations or errors in retention management.

**12. Monitoring and Biannual Review**

• Conduct biannual audits of record retention schedules and destruction actions.

• Validate that expired records have been properly destroyed.

• Identify exceptions or deviations and implement corrective actions.

• Update retention schedules and practices based on regulatory changes or operational needs.

**13. Incident Response**

• Record-related incidents (unauthorized access, accidental deletion, incomplete destruction) must be immediately reported.

• Investigate incidents to determine root cause and prevent recurrence.

• Apply corrective actions, including retraining, process adjustments, or system updates.

• Document all incidents and resolutions for governance review.

**14. Continuous Improvement and Enforcement**

• Review the policy annually or after significant incidents or regulatory changes.

• Enforcement actions may include retraining, restricted access, or disciplinary measures for non-compliance.

• Promote a culture of accountability and proactive record management across all personnel.

• Maintain a clear audit trail of all retention and destruction activities for corporate and regulatory review.