Data Handling, Destruction & Retention Standard

*Revision: r1.0*

*Effective Date: ddmmyyyy*

*Classification: Internal*

**Internal INFORMATION**

This is a proprietary document and is the property of XXXX; it contains information that is proprietary, or otherwise restricted from disclosure. If you are not an authorised recipient, please return this document to the above-named owner(s). Dissemination, distribution, copying or use of this document in whole or in part by anyone other than the intended recipient is strictly prohibited without prior written permission of XXXX.

Table of Contents

1. Introduction 4

1.1 Document Definition 4

1.2 Objective 4

1.3 Scope 4

1.3.1 Applicability to employees 4

1.3.1 Applicability to External Parties 4

1.3.2 Applicability to Assets 4

1.4 Related Documents / References 4

2. Standard Statements 5

Data Handling and Destruction Requirements 5

2.1 Access Controls 5

2.2 Copying/Printing (applies to both paper and electronic forms) 5

2.3 Network Security 6

2.4 System Security 6

2.5 Virtual Environments 6

2.6 Physical Security 6

2.7 Remote Access 7

2.8 Data Storage 7

2.9 Transmission 7

2.10 Transfer Agreements 7

2.11 Confidentiality & Non-Disclosure Agreements 7

2.12 Auditing 7

2.13 Log Monitoring 8

2.14 Backup/Disaster Recovery 8

2.15 Media Distribution 8

2.16 Media Storage 8

2.17 Media Inventories 8

2.18 Media Destruction (hard drives, CDs, DVDs, tapes, paper, etc.) 8

2.19 Training 8

2.20 Mobile Devices 8

2.21 Electronic Data, Files and Folders destruction 8

3. Data Retention 9

4. Standard Compliance & Enforcement 11

4.1 Compliance Measures 11

4.2 Enforcement 12

5. Exception Process / Glossary 13

5.1 Exception Process 13

5.2 Glossary / Acronyms 13

6. Document Management 14

6.1 Document Revision Log 14

6.2 Document Ownership 14

6.3 Document Coordinator 14

6.4 Document Approvers 14

6.5 Distribution 14

# Introduction

## Document Definition

This document is a Standard.

For a full description of document types, see *XXXX-POL-ALL-001 - Information Security Policy Framework*.

## Objective

The objective of this standard is to provide information security requirements for the handling, destruction and retention of XXXX data assets.

In the context of this Standard, “data asset” and “information asset” are used interchangeably.

An information asset is a definable piece of data, regardless of format, which is recognised as valuable to the organisation. Information assets may include but are not limited to all forms and types of business proprietary information/content, customer related information, financial, strategies and processes, analytics, innovation, legal and employees/personnel data.

## Scope

### Applicability to employees

XXXX refers to XXXX as well as its majority-owned subsidiaries and joint ventures (if applicable). This standard applies to all employees, officers, members of Board of Directors, and all consultants, and contractors.

### Applicability to External Parties

Relevant standard statements will apply to any external party and be included in contractual obligations on a case-by-case basis.

### Applicability to Assets

This standard applies to all information assets globally owned by XXXX, or where XXXX has custodial responsibilities.

## Related Documents / References

* *XXXX-POL-ALL-001 - Information Security Policy Framework*
* *XXXX-POL-ALL-004 - Data Classification Policy*
* *XXXX-POL-ALL-005 – Data Handling and Retention Policy*
* *XXXX-POL-ALL-025 – Information Disposal Policy*

# Standard Statements

## Data Handling and Destruction Requirements

The following table defines required safeguards for protecting data and data collections based on their classification above the level of Public. In addition to the following data security standards, any data covered by regional or country laws or regulations or contractual agreements must meet the security requirements defined by those laws, regulations, or contracts:

|  |  |  |  |
| --- | --- | --- | --- |
| **SECURITY CONTROL CATEGORY** | **DATA CLASSIFICATION** | | |
| **Internal** | **Confidential** | **Restricted** |
| Access Controls | * No restriction for viewing * Authorisation by Data Owner or designee required for modification; supervisor approval also required if not a self-service function | * Viewing and modification restricted to authorised individuals as needed for business-related roles * Data Owner or designee grants permission for access, plus approval from supervisor * Authentication and authorisation required for access * If session has been idle for more than 10 minutes, require the user to re-authenticate to re-activate the terminal or session | * Viewing and modification restricted to authorised individuals as needed for business-related roles * Data Owner or designee grants permission for access, plus approval from supervisor * Authentication and authorisation required for access * Confidentiality agreement required * If session has been idle for more than 10 minutes, require the user to re-authenticate to re-activate the terminal or session |
| Copying/Printing (applies to both paper and electronic forms) | * No restrictions | * Data should only be printed when there is a legitimate need * Copies must be limited to individuals with a need to know * Data should not be left unattended on a printer/fax * Data may be sent via regular mail | * Data should only be printed when there is a legitimate need * Copies must be limited to individuals authorised to access the data and have signed a confidentiality agreement * Data should not be left unattended on a printer/fax * Copies must be labelled “Restricted” * Must be sent via a registered courier with confirmation of receipt by recipient provided after delivery |
| Network Security | * May reside on a public network * Protection with a firewall recommended * IDS/IPS protection recommended * Protection only with router ACLs acceptable | * Protection with a network firewall required * IDS/IPS protection required * Protection with router ACLs optional * Servers hosting the data should not be visible to Internet * May be in a shared network server subnet with a common firewall rule-set for the set of servers | * Protection with a network firewall using "default deny" rule-set required * IDS/IPS protection required * Protection with router ACLs optional * Servers hosting the data cannot be visible to the entire Internet, nor to untrusted * Must have a firewall rule-set dedicated to the system * The firewall ruleset should be reviewed annually |
| System Security | * Must follow general best practices for system management and security * Host-based software firewall recommended | * Must follow XXXX specific and OS-specific best practices for system management and security * Host-based software firewall required * Host-based software IDS/IPS recommended | * Must follow XXXX specific and OS-specific best practices for system management and security * Host-based software firewall required * Host-based software IDS/IPS recommended |
| Virtual Environments | * May be hosted in a virtual server environment * All other security controls apply to both the host and the guest virtual machines | * May be hosted in a virtual server environment * All other security controls apply to both the host and the guest virtual machines * Should not share the same virtual host environment with guest virtual servers of other security classifications | * May be hosted in a virtual server environment * All other security controls apply to both the host and the guest virtual machines * Cannot share the same virtual host environment with guest virtual servers of other security classifications |
| Physical Security | * System must be locked or logged out when unattended * Host-based software firewall recommended | * System must be locked or logged out when unattended * Hosted in a secure location required; a Secure Data Centre is recommended | * System must be locked or logged out when unattended * Hosted in a Secure Data Centre required * Physical access must be monitored, logged, and limited to authorised individuals 24x7 |
| Remote Access | * No restrictions | * Access restricted to local network or VPN Remote access by third party for technical support limited to authenticated, temporary access via direct dial-in modem or secure protocols over the Internet | * Restricted to local network or secure VPN/Citrix group * Unsupervised remote access by third party for technical support not allowed * Two-factor authentication recommended |
| Data Storage | * Storage on a secure server recommended * Storage in a secure Data Centre recommended | * Storage on a secure server recommended Storage in a secure Data Centre recommended * Should not store on an individual's workstation or a mobile device | * Storage on a secure server required * Storage in Secure Data Centre required * Should not store on an individual workstation or mobile device (e.g., a laptop computer); if stored on a workstation or mobile device, must use whole-disk encryption * Encryption on backup media required * Paper/hard copy: do not leave unattended where others may see it; store in a secure location |
| Transmission | * No restrictions | * Encryption required (for example, via TLS or secure file transfer protocols) * Cannot transmit via e-mail unless encrypted and secured with a digital signature | * Encryption required (for example, via TLS or secure file transfer protocols) * Cannot transmit via e-mail unless encrypted and secured with a digital signature |
| Transfer Agreements | * Contractual restrictions with external parties recommended | * Contractual restrictions with external parties and compliance with GDPR recommended | * Contractual restrictions with external parties and compliance with GDPR required |
| Confidentiality & Non-Disclosure Agreements | * Mutual Non-Disclosure Agreement (MNDA) or other equivalent confidentiality agreement recommended. | * Mutual Non-Disclosure Agreement (MNDA) or other equivalent confidentiality agreement recommended. | * Mutual Non-Disclosure Agreement (MNDA) or other equivalent confidentiality agreement must be in place. |
| Auditing | * Not needed | * All use and failure of authentication mechanisms * All actions taken with privileged access * All access to confidential data | * All use and failure of authentication mechanisms * All actions taken with privileged access * All access to restricted data |
| Log Monitoring | * Standard log monitoring practices | * Enhanced log monitoring recommended * 9X5X365 alerting to Incident Response Team | * Real-time log monitoring required * 24X7X365 alerting to Incident Response Team |
| Backup/Disaster Recovery | * Backups required; daily backups recommended | * Daily backups required * Off-site storage recommended | * Daily backups required * Off-site storage in a secure location required |
| Media Distribution | * No restrictions | * Tracked against all internal and external distribution to organisations and individuals | * Tracked against all internal and external distribution to organisations and individuals |
| Media Storage | * No restrictions | * Storage containers used for materials that are to be destroyed must be secured | * Storage containers used for materials that are to be destroyed must be secured |
| Media Inventories | * Not required | * Annual | * Annual |
| Media Destruction (hard drives, CDs, DVDs, tapes, paper, etc.) | * No restrictions | * Paper documents should be disposed of in confidential waste bins or cross-cut shredded. * Wipe/erase media is performed securely | * Cross-shred in confidential waste bin or incinerate paper and write-once media * Destruction of all other physical media per accepted industry standards (e.g. NIST SP800-88) |
| Training | * General security awareness training recommended | * General security awareness training required * Data security training required | * General security awareness training required * Data security training required * Applicable policy and regulation training required |
| Mobile Devices | * Password protection recommended; locked when not in use | * Password protected, locked when not in use | * Password protected, locked when not in use, * Encryption used for restricted data |
| Electronic Data, Files and Folders destruction | * No restrictions | * Delete/erase including from recycle bin * Drop/delete tables, views and associated indexes | * Delete/erase including from recycle bin * Use Eraser/Microsoft Sdelete to overwrite severally and delete * Drop/delete tables, views and associated indexes |

# Data Retention

* It is the policy of XXXX to preserve all Records for the period of their immediate or current use, unless a longer retention period is necessary for historical reference or to comply with contractual or legal requirements.
* To provide for consistent retention and disposal of common XXXX Records, **Exhibit A- Retention Schedule** is provided in this standard document and defines a retention schedule that meets XXXX’s business, legal, fiscal, and reference requirements
* Records that serve no useful purpose should be promptly and systematically deleted and destroyed, with the exception of documents that are relevant to or discoverable in pending or potential litigation and other legal and official proceedings.
* Electronic files and documents will be retained as if they were paper documents. Any electronic files which fall into one of the document categories listed in Exhibit A will be maintained for the appropriate period of time
* XXXX employees, officers, and directors shall not knowingly alter, conceal, or destroy a Record with the intent to impede, obstruct or influence an investigation or proper administration of any matter within the jurisdiction of any department or agency of the United Kingdom government or in relation to or contemplation of any such matter or case**.**
* Unless specified otherwise in this standard, the retention period for a Record begins on the date that the Record was received or created by XXXX**.**
* The retention period for Records related to a Court hearing or a compliance violation investigation begins upon the end date of the hearing or compliance violation investigation**.**
* Immediately upon learning of an investigation or court proceeding involving a particular XXXX matter or subject, XXXX (Legal Services) shall notify all employees to preserve all Records pertaining to that matter or subject and to cease and avoid any destruction of the Records pertaining to that matter or subject that would otherwise be authorized by this record retention and destruction policy. In such a case, the retention period for such Records will be specified by the XXXX Legal department.
* Records whose retention period is explicitly stated within this standard or have a retention period defined by the XXXX Legal department, must be destroyed within six (6) months of the end date of the Record’s retention period. Records whose retention period is not explicitly defined and is subject to interpretation of immediate or current use must be destroyed within a period of six (6) months from the end date of its immediate or current use, or two (2) years after the Record was created or received. Upon identifying Records whose immediate or current use exceeds two (2) years which are not explicitly defined in this policy, XXXX should consider adding such Records retention period to this Policy.

**Exhibit A – Retention Schedule**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Record Type** | **1 year** | **2 years** | **3 years** | **7 years** | **Permanent** |
| Accounts payable ledgers & schedules |  |  |  | **Y** |  |
| Accounts receivable ledgers & schedules |  |  |  | **Y** |  |
| XXXX policy and practice manuals |  |  |  |  | **Y** |
| Audit reports |  |  |  |  | **Y** |
| XXXX statements |  |  |  | **Y** |  |
| XXXX reconciliations |  |  |  | **Y** |  |
| Cancelled checks |  |  |  | **Y** |  |
| Chart of accounts |  |  |  |  | **Y** |
| Contracts & leases: |  |  |  |  |  |
| * Current |  |  |  |  | **Y** |
| * Expired |  |  |  | **Y** |  |
| Corporate records: |  |  |  |  |  |
| * Board and Committee Meeting Agendas and Minutes |  |  |  |  | **Y** |
| * Subcommittee, Work Group, and Task Force Agendas and Minutes |  |  |  | **Y** |  |
| * Charters |  |  |  |  | **Y** |
| * Bylaws |  |  |  |  | **Y** |
| * Articles of Incorporation |  |  |  |  | **Y** |
| * Annual Reports |  |  |  |  | **Y** |
| Correspondence: |  |  |  |  |  |
| * Contributions |  |  |  | **Y** |  |
| * General |  |  |  | **Y** |  |
| * Legal & important matters only |  |  |  |  | **Y** |
| Routine vendor | **Y** |  |  |  |  |
| Depreciation schedules |  |  |  |  | **Y** |
| Election records |  |  |  |  | **Y** |
| Employee personnel records  (after termination) |  |  |  | **Y** |  |
| Employee payroll tax returns |  |  |  | **Y** |  |
| Employment applications |  | **Y** |  |  |  |
| Financial records/schedules used in preparation of tax returns (from date return filed) |  |  |  |  | **Y** |
| Financial statements (year-end; other months optional) |  |  |  |  | **Y** |
| General ledgers: year-end trial balances |  |  |  | **Y** |  |
| Insurance policies (including expired policies |  |  |  |  | **Y** |
| Inventories |  |  |  | **Y** |  |
| Invoices: |  |  |  |  |  |
| * From vendors |  |  |  | **Y** |  |
| * To customers |  |  |  | **Y** |  |
| Ownership of property, real estate, patents, trademarks, copyrighted documents (from date ownership ends) |  |  |  | **Y** |  |
| Payroll records & summaries |  |  |  | **Y** |  |
| Pension documents & records |  |  |  |  | **Y** |
| Petty cash vouchers |  |  |  | **Y** |  |
| Purchase orders |  |  |  | **Y** |  |
| Receipt records (sales, etc.) |  |  |  | **Y** |  |
| Sales records and journals |  |  |  | **Y** |  |
| Subsidiary ledgers |  |  |  | **Y** |  |
| Tax returns |  |  |  |  | **Y** |
| Vouchers for payments to employees for reimbursements, allowances, etc. |  |  |  | **Y** |  |
| Emails |  |  |  | **Y** |  |
| Customer record |  |  |  | **Y** |  |
| Active/ Dormant Account |  |  |  |  | **Y** |
| Closed Account | **Y** |  |  |  |  |
| Card Holder Information (PAN,  Expiry Date etc.) |  |  |  | **Y** |  |
| Camera Data | At least 30 days |  |  |  |  |
| Instant Message | 90 days |  |  |  |  |

# Standard Compliance & Enforcement

## Compliance Measures

If applicable, compliance with the above Standard can be measured by the following criteria. Example evidence will vary depending on any supporting guidelines implemented to support this Standard. The following list is not exhaustive, and all example evidence types may not be required to validate compliance.

Evidence of compliance can be presented in hard copy or electronic format.

|  |  |
| --- | --- |
| **Criteria** | **Example Evidence** |
| For a selection of XXXX information assets, verify evidence of data ownership. | * Information asset (e.g., application) inventory listing, including asset owners * Output from asset management tools / systems * Output from risk assessment (e.g., Governance, Risk and Compliance – GRC) tools |
| For a selection of XXXX information assets, obtain evidence of documented information classifications. | * Information asset (e.g., application) inventory listing, including asset owners * Output from asset management tools / systems * Output from risk assessment (e.g., Governance, Risk and Compliance – GRC) tools |
| For a selection of XXXX information assets, verify that information labelling and handling requirements are implemented. | * Evidence of the risk assessment process, including labelling and handling * Root cause analysis from internal or external audits |
| For a selection of XXXX information assets, obtain evidence that information classifications are reviewed on a periodic basis. | * Physical sign-off of asset inventory listing * Electronic sign-off via asset inventory, GRC tools, email, etc. |

## Enforcement

All staff of XXXX must comply with all Information Security Standards. Failure to comply with these standards may result in disciplinary action in accordance with the current XXXX Human Resources policy. Disciplinary actions may include, but are not limited to:

* verbal and/or written warnings;
* instant dismissal; and
* actions by judicial and regulatory authorities.

# Exception Process / Glossary

## Exception Process

Non-compliance with the Standard statements described in this document must be reviewed and approved in accordance with the Exception Process defined in *XXXX-POL-ALL-001 - Information Security Policy Framework*.

## Glossary / Acronyms

|  |  |
| --- | --- |
| MNDA | Mutual Non-Disclosure Agreement |

# Document Management

## Document Revision Log

|  |  |  |  |
| --- | --- | --- | --- |
| **Date** | **Editor** | **Revision #** | **Description of Change** |
|  |  |  |  |

## Document Ownership

This Standard is owned by the YYYY

## Document Coordinator

This Standard is coordinated by the YYYY

## Document Approvers

|  |  |  |
| --- | --- | --- |
| **Approver Name** | **Signature** | **Date** |
|  |  |  |

## Distribution

Distribution is to all staff