Project Information Security Requirements

*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. Procedure Statements 6

2.1 Information Security Requirement Summary 6

3. Asset Protection – Minimum Control Requirements 8

4. Change and Patch Management – Minimum Control Requirements 9

5. Cloud and Internet Computing – Minimum Control Requirements 9

6. Information Security Risk Management – Minimum Control Requirements 10

7. Malware Protection – Minimum Control Requirements 12

8. Network Security – Minimum Control Requirements 13

9. Secure Development – Minimum Control Requirements 14

10. Security Assessment – Minimum Control Requirements 15

11. System Configuration – Minimum Control Requirements 17

12. System Monitoring – Minimum Control Requirements 18

13. Right of Inspection – Minimum Control Requirements 19

14. XXXX Dedicated Space – Control Requirements 19

15. Cryptography– Minimum Control Requirements 23

16. Procedure Compliance & Enforcement 26

16.1 Compliance Measures 26

16.2 Enforcement 26

17. Glossary / Acronyms 27

17.1 Glossary / Acronyms 27

18. Document Management 28

18.1 Document Revision Log 28

18.2 Document Ownership 28

18.3 Document Coordinator 28

18.4 Document Approvers 28

18.5 Distribution 28

# Introduction

## Document Definition

This document is a Procedure.

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

## Objective

This procedure covers information security requirements for new projects, acquisitions, and suppliers. This document should be used in conjunction with the Outsourcing and Supplier Policy and *XXXX-STD-ALL-022 - Vendor Due Diligence Standard and XXXX-STD-ALL-023- Project Management Framework*

.

## Scope

### Applicability to employees

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

### Applicability to External Parties

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

### Applicability to Assets

This procedure 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*
* *Outsourcing and Supplier Policy V1.1.*
* *XXXX-STD-ALL-022 - Vendor Due Diligence Standard*
* *XXXX-STD-ALL-023- - Project Management Framework*

# Procedure Statements

## Information Security Requirement Summary

|  |  |  |
| --- | --- | --- |
| **Information Security Requirement** | **Description** | **Why this is important** |
| 1. Asset Protection and System Configuration | XXXX Data and the assets or systems storing or processing it must be protected against physical tampering, loss, damage or seizure and inappropriate configuration or changes. | If this principle is not implemented, inappropriately protected XXXX Data could be compromised, which may result in legal and regulatory sanction, or reputational damage. Also, services may be vulnerable to security issues which could compromise XXXX Data, cause loss of service or enable other malicious activity. |
| 2. Change and Patch Management | XXXX Data and the systems storing or processing it, must be protected against inappropriate changes which could compromise availability or integrity. | If this principle is not implemented, services may be vulnerable to security issues which could compromise consumer data, cause loss of service or enable other malicious activity. |
| 3. Cloud / Internet Computing | XXXX Data stored in the cloud or on a public facing internet connection must be adequately protected via appropriate controls to prevent data leakage. | If this principle is not implemented inappropriately protected XXXX Data could be compromised, which may result in legal and regulatory sanction, or reputational damage. |
| 4. Information Security Risk Management | XXXX Data and critical infrastructure must be adequately protected via appropriate people, processes and technology controls to prevent disruption of service or loss of data following Information attacks. | If this principle is not implemented, then XXXX information may be disclosed and / or there may be loss of service leading to legal and regulatory sanction, or reputational damage. |

|  |  |  |
| --- | --- | --- |
| 5. Malware Protection | Anti-malware controls and tools must be in place to adequately protect against malicious software such as viruses and other forms of malware. | If this principle is not implemented, then XXXX information may be disclosed leading to legal and regulatory sanction, or reputational damage. |
| 6. Network Security | All external and internal networks as part of the service must be identified and have appropriate protections to defend against attacks through them. | If this principle is not implemented, external or internal networks could be subverted by attackers in order to gain access to the service or data within it. |
| 7. Secure Development | Services and systems including mobile applications must be designed and developed to mitigate and protect against vulnerabilities and threats to their security. | If this principle is not implemented, services may be vulnerable to security issues which could compromise consumer data, cause loss of service or enable other malicious activity. |
| 8. Security Assessment | Systems and services must be independently and rigorously tested for vulnerabilities. | If this principle is not implemented, then XXXX information may be disclosed and / or loss of service may occur leading to legal and regulatory sanction, or reputational damage. |
| 9. Systems Monitoring | Monitoring and auditing and logging of systems must be in place to detect inappropriate or malicious activity. | If this principle is not implemented, suppliers will not be able to detect and respond to inappropriate or malicious use of their service or data within reasonable timescales. |
| 10. XXXX Dedicated Space | For services provided which require formal XXXX Dedicated Space (BDS) i.e disaster recovery site, specific BDS physical and technical requirements must be in place. | If this principle is not implemented, appropriate physical and technical controls may not be in place leading to service delays or disruption or Information Security Breaches occurring. |
| 11. Cryptography | Confidential and XXXX Data must be encrypted. | If this principle is not implemented, appropriate physical and technical controls may not be in place leading to service delays or disruption or Information Security Breaches occurring. |

# Asset Protection – Minimum Control Requirements

|  |  |  |
| --- | --- | --- |
| **Control Area** | **Control Title** | **Control Description** |
| IT Asset Management | Inventory | An Inventory of all appropriate IT assets must be in place and there must be at least one test annually to validate that the IT asset inventory is current, complete and accurate |
| IT Asset Management | Backup media | All backup and archival media containing XXXX information used to provide the Services, must be encrypted and contained in secure, environmentally-controlled storage areas owned, operated, or contracted for by the Supplier and in line with the Information Classification and Handling Schedule. |
| IT Asset Management | Secure Data / Media Disposal | XXXX Data / Confidential Information that is printed/written on paper must be destroyed securely as soon as it is no longer required. Data that is on media that is no longer required must be securely wiped so that information cannot be retrieved |
| IT Asset Management | Mobile Computing | The use of mobile computing must be configured securely at all times as per business usage of mobile devices policies and procedures to prevent data Leakage and misuse |

# Change and Patch Management – Minimum Control Requirements

|  |  |  |
| --- | --- | --- |
| **Control Area** | **Control Title** | **Control Description** |
| Change and Patch Management | Change Management | All key IT changes prior to implementation must be logged, tested and approved via an approved, robust change management process to prevent any service disruption or security breaches |
| Change and Patch Management | Emergency Fixes | The XXXX shall ensure that Emergency Fixes are implemented when available and approved unless this introduces higher business risks. Supplier Systems that for any reason cannot be updated shall have security measures installed to fully protect the vulnerable system. All changes must be undertaken in accordance with the XXXX’s change management process. |
| Change and Patch Management | Patch Management | * The XXXX shall develop and implement a patch management strategy that is supported by management controls and supported by patch management procedures and operational documentation. * As soon as they become available, IT Security patches and security vulnerability updates must be installed through an approved process in a timely manner to prevent any security breaches. All changes must be undertaken in accordance with the approved change management process. * Open source applications are checked for outstanding vulnerabilities |

# Cloud and Internet Computing – Minimum Control Requirements

|  |  |  |
| --- | --- | --- |
| **Control Area** | **Control Title** | **Control Description** |
| Cloud Computing | Cloud Computing | All use of cloud computing used as part of the service to XXXX must be approved by change management board and controls to protect data and the service must be commensurate with the risk profile to prevent data leakage and Information breaches. |
| Cloud Computing | Cloud Computing | * Assets must be located inside approved countries / locations including the disaster recovery locations. * Asset information much be captured including the virtual systems used to provide cloud services. Assets must be protected with DLP requirements, Anti-Virus, HIDS, NIDS, HD encryption, Cryptographic controls. A prior formal agreement for data transfer into cloud environments, portable storage, etc. must be in place for all the data classified and data inventories. * Backup media – must be encrypted. The encryption keys need to be secured and access restricted * All controls related to cloud services must be discussed and agreed with XXXX. |

# Information Security Risk Management – Minimum Control Requirements

|  |  |  |
| --- | --- | --- |
| **Control Area** | **Control Title** | **Control Description** |
| Information Security Risk Management | Information Risk Assessment | The Information security risk profile to the organizational operations, assets, and individuals must be understood by   * Assessing asset vulnerabilities * Identifying both internal and external threats * Assessing potential business impacts   Risks and threats must be identified, prioritized and action taken accordingly to mitigate. This shall be factored in for all new projects and acquisitions. For Supplier systems, the Supplier shall undertake regular Risk Assessments in relation to information security (and in any event not less than once every 12 months) and shall implement such controls and take such steps as are required to mitigate the risks identified. If a material risk identified that could adversely affect the reputation or service provided to XXXX, the supplier must notify XXXX within 24 hours. |
| Information Security Risk Management | Information Security Governance | Appropriate Information security governance must be in place by ensuring that:   * All new projects and acquisitions have a process for integrating information security into the development * A specialist Information / Information security function which has responsibility for integrating   information security consistently into the Supplier’s business is in place   * The policies, procedures, and processes to manage and monitor the supplier’s regulatory, legal, Information risk, environmental, and operational requirements are understood, documented and in place and approved by Senior Management on an annual basis * The Supplier shall ensure that the information security status of critical IT environments (including the Supplier Systems), applications, computer installations, networks and systems development activity supporting the Services shall be subject to thorough and regular security audits/reviews conducted by an independent function within the Supplier’s organization. If a material vulnerability is identified that could adversely affect the reputation or service provided to XXXX, the supplier must notify XXXX within 24 hours. |

|  |  |  |
| --- | --- | --- |
| Information Security Risk Management | Roles and responsibilities | * The XXXX must regularly and in any event not less than once in every calendar year during the term, measure, review and document its compliance with information security compliance checklist * Without prejudice to XXXX other rights and remedies, XXXX may risk assess any non- compliance reported by the Supplier to XXXX and may provide a timeframe within which the Supplier shall complete any reasonably required remediation. |
| Information Security Risk Management | Incident Response | For Supplier systems, Security incidents and data breaches must be responded to and reported to XXXX immediately and progress on remedial actions. An incident response process for timely handling and reporting of intrusions involving XXXX data and/or services used by XXXX must be established. This must also include an appropriate approach to forensic investigations |
| Information Security Risk Management | Awareness Training | Appropriate training material including Information security awareness and ensures that all relevant employees are suitably trained to carry out their roles and responsibilities |

# Malware Protection – Minimum Control Requirements

|  |  |  |
| --- | --- | --- |
| **Control Area** | **Control Title** | **Control Description** |
| Malware Protection | Malware Protection | The most up to date Malware protection must always be applied to all IT Assets used to provide the service to prevent service disruption or security breaches   * The XXXX shall establish and maintain up-to-date protection against Malicious Code / Malware in accordance with XXXX-POL-ALL-014 - Vulnerability Management Policy for all new projects and acquisitions * The Supplier shall protect against transferring Malicious Code to XXXX systems, XXXX customers and other Third Parties using XXXX Systems or Supplier Systems using current industry standard methods. |

# Network Security – Minimum Control Requirements

|  |  |  |
| --- | --- | --- |
| **Control Area** | **Control Title** | **Control Description** |
| Network Security | External connections | * The XXXX shall ensure that its network shall be designed and implemented to be able to cope with current and predicted levels of traffic and shall be protected using all available in-built security controls when implementing new projects and acquisitions * The Supplier shall ensure that its network related to the provision of the Service shall be supported by accurate, up-to-date diagrams that include all system components and interfaces to other systems and be supported by documented control requirements and procedures. * All external connections to the network must be documented, routed through a firewall and verified and approved prior to the connections being established to prevent data security breaches |

|  |  |  |
| --- | --- | --- |
| Network Security | Wireless access | All wireless access to the network must be subject to authorization, authentication, segregation and encryption protocols ex. WPA2 to prevent security breaches.  Any Wireless connection shall only be permitted from supplier locations must be approved by XXXX |
| Network Security | Firewalls | * The XXXX shall ensure the implementation of new projects and acquisitions is consistent with the existing firewall rules and security. * Firewalls must ensure secure connections between internal and external systems and shall be configured as so to only allow the required traffic to pass through. Firewall configurations must be regularly reviewed to remove redundant or inappropriate rules and applicable sign off available to evidence. |
| Network Security | Intrusion detection / prevention | Intrusion detection and prevention tools and systems must be deployed at all appropriate locations on the network and output monitored accordingly to detect for Information security breaches including Advanced Persistent Threats (APTs). |
| Network Security | Distributed Denial of Service (DDoS) | A defense in depth approach must always be implemented in the network and new projects to protect against service interruption via Information attacks. This includes Denial of Service (DoS) and Distributed Denial of Services (DDoS) attacks. |

# Secure Development – Minimum Control Requirements

|  |  |  |
| --- | --- | --- |
| **Control Area** | **Control Title** | **Control Description** |
| Secure Development | Secure development methodology | All development must always be undertaken in line with the approved documented Systems Development Methodology. Secure coding standards must be in place and adopted in line with XXXX-POL-ALL-019 - Secure Application Development Policy to prevent security vulnerabilities and service interruptions. |
| Secure Development | Environment segregation | All systems development/build must always be undertaken in a non-production environment and segregation of duty enforced to prevent data leakage and accidental data modification/deletion. There must be no live data in test unless approved by the change management board. |
| Secure Development | Live Data in Non- Production Environments | For new projects and Supplier systems, the XXXX shall ensure that live data (including Personal Data) will not be used within non-production environments without change management board prior written approval and agreement of the controls to be implemented to protect that live data. Where live data is used in non-production environments then the testing team shall ensure that it must be secured to the same extent as the production environment. |
| Secure Development | Secure Coding Practices | New projects and Supplier systems shall have secure development practices in place, including the definition and testing of security requirements. Such practices shall be fully documented. |
| Secure Development | Segregation of Duties | The XXXX shall ensure that segregation of duties is in place for system development, including ensuring that system developers do not have access to the live environment, unless in an emergency where such access would be protected with adequate controls such as break-glass procedures. Such activities in these circumstances shall be logged and subject to independent review. |
| Secure Development | Quality assurance | The quality assurance function must check that all the key security activities have been incorporated into the system development process to prevent service interruptions and security vulnerabilities |

# Security Assessment – Minimum Control Requirements

|  |  |  |
| --- | --- | --- |
| **Control Area** | **Control Title** | **Control Description** |
| Security Assessment | Penetration test | * The XXXX shall engage an independent IT security assessment / Penetration Test of the IT infrastructure including Disaster Recovery sites. This must be undertaken at least annually to identify vulnerabilities that could be exploited to breach the privacy of XXXX Data through Information Attacks. All vulnerabilities must be prioritized and tracked to resolution. The test must be undertaken in line with XXXX-POL-ALL-014 - Vulnerability Management Policy and by a recognized Security Assessment Vendor. * Security Assessment Vendor shall inform and agree on scope of security assessment with XXXX and test activities, in particular start and end date/times to allow any events raised by XXXX monitoring systems. Also, to prevent disruption to key XXXX activities such as end of year finance reports etc. * XXXX and/or its Agents shall have the right to conduct a Security Assessment of the Supplier Systems |

**Security Assessment** means tests performed on the Supplier Systems/New Projects in order to:

* 1. identify design and/or functionality issues in applications or infrastructure.
  2. probe for weaknesses in applications, network perimeters or other infrastructure elements as well as weaknesses in process or technical countermeasures.
  3. identify potential vulnerabilities that may result from poor or improper system configuration, known and/or unknown hardware or software flaws including, but not limited to, the following examples for infrastructure and application testing which could expose the Supplier and XXXX to risks from malicious activities;
     1. invalidated or unsanitised input.
     2. broken access control.
     3. broken authentication and session management.
     4. cross-site scripting (XSS) flaws.
     5. buffer overflows.
     6. injection flaws.
     7. improper error handling.
     8. insecure storage.
     9. denial of service.
     10. insecure configuration management.
     11. proper use of SSL/TLS.
     12. proper use of encryption; and
     13. anti-virus reliability and testing,

This assessment will typically incorporate activities also commonly referred to as penetration testing.

**Security Assessment Vendor** means a suitably qualified Third Party employed to perform a Security Assessment.

# System Configuration – Minimum Control Requirements

|  |  |  |
| --- | --- | --- |
| **Control Area** | **Control Title** | **Control Description** |
| System Configuration | System Time | All devices and systems must have correct and consistent time at all times to prevent system errors and also to ensure activities can be forensically investigated. |
| System Configuration | Remote Access | All remote access to systems must be authorized and approved by XXXX prior to access being established to prevent security breaches. Remote access must be via multi factor authentication. User activity shall be logged and subject to review. |
| System Configuration | Secure Build | Host systems and network devices forming part of the new acquisition/ Supplier Systems must be configured to function in accordance with XXXX-POL-ALL-018 - Network Configuration Policy and XXXX-POL-ALL-014 - Vulnerability Management Policy, applicable specifications and functionality requirements to prevent unauthorized or incorrect updates being applied to such systems and network devices |

# System Monitoring – Minimum Control Requirements

|  |  |  |
| --- | --- | --- |
| **Control Area** | **Control Title** | **Control Description** |
| System Monitoring | Log Management | All key systems including key applications must be set to log key events. Logs must be centralized, appropriately secured and kept for a minimum of 12 months. The key events must be those that have the potential to impact the confidentiality, integrity and availability of the Service to XXXX and that may assist in the identification or investigation of material incidents and/or breaches of access rights occurring in relation to the Supplier Systems.  The system must record and monitor the following as a minimum:   1. User identification 2. Type of event 3. Date and Time 4. Success or failure indication 5. Origination of event 6. Identity or name of affected data, system component, or resource. 7. Administrator activities |
| System Monitoring | Log Review | Logs from new systems must be in a format readily available for review for potential Information Security breaches / fraudulent activity. Event data must be collected and correlated from multiple sources and sensors. Detected events must be analyzed to understand attack targets and methods. Upon identification of any material incidents and/or breaches of access rights shall ensure that the Incident Management Process is followed |

# Right of Inspection – Minimum Control Requirements

|  |  |  |
| --- | --- | --- |
| **Control Area** | **Control Title** | **Control Description** |
| Right of Inspection | XXXX Right of Inspection | For supplier managed systems XXXX may, conduct a security review of any site being used by or required to be used by the Supplier or its Sub-contractors to develop, test, enhance, maintain or operate the Supplier Systems used in the provision or recovery of the Services in order to review the Supplier’s compliance with its obligations. XXXX may also carry out an inspection immediately after a Security Incident. This will be included in the SLA with the Supplier  Any non-compliance identified by XXXX during an inspection shall be risk assessed by XXXX and XXXX shall specify a timeframe within which the Supplier shall complete any required remediation and the Supplier shall complete any required remediation within that timeframe. The Supplier shall provide all assistance reasonably requested by XXXX in relation to any inspection. |

# XXXX Dedicated Space – Control Requirements

|  |  |  |
| --- | --- | --- |
| **Control Area** | **Control Title** | **Control Description** |
| XXXX Dedicated Space | Physical Separation | The physical area occupied must be dedicated to XXXX and not shared with other companies / vendors. |
| XXXX Dedicated Space | Physical Access Control | Secure automatic controls must be operating for access to BDS including: |

|  |  |  |
| --- | --- | --- |
|  |  | 1. If for authorized staff;    1. Photo ID badge/lanyard which is visible at all times    2. proximity card readers are implemented    3. Anti-pass back mechanism is enabled 2. Visitor/vendor controls    1. Sign in log book    2. Limited use badge which is visible at all times |
| XXXX Dedicated Space | Physical Access Control | Alarms must be configured to report through a centralized access system with auditable access control |
| XXXX Dedicated Space | Physical Access Control | Monitor the controls ensuring appropriate access is granted to the BDS and other critical areas |
| XXXX Dedicated Space | House Keeping | Only authorized housekeeping and support staff like electricians, AC maintenance, house-keeping etc. must be allowed in the BDS |
| XXXX Dedicated Space | Environmental Controls | Controls must be implemented to protect against environmental factors for example fire, flood, hurricane, tornado, pestilence, infestations, humidity, temperature, dust, food & drink contamination |
| XXXX Dedicated Space | Media Handling | Access to all media pertaining or relating to the services delivered to XXXX must be strictly controlled and authorized |

|  |  |  |
| --- | --- | --- |
| XXXX Dedicated Space | Remote Access - ID&V | Every individual user must only authenticate to the XXXX network from the BDS using a XXXX authentication details and a provided multi factor authentication token |
| XXXX Dedicated Space | Remote Access - Software Tokens | Installation of any encryption software and soft tokens must be done by XXXX administrators within the approved BDS on assigned desktops |
| XXXX Dedicated Space | Remote Access - Out of Office Support | Remote access to BDS environment is not provided by default for out of office hours/out of business hours support. Any remote access must be approved by XXXX |
| XXXX Dedicated Space | Email and Internet | Network connectivity must be securely configured to block email and unapproved internet activity on the vendor's network |
| XXXX Dedicated Space | System and Desktops | Secure desktop builds must be configured to industry best practice for computers within the BDS |
| XXXX Dedicated Space | System and Desktops | Generic or shared or privilege access accounts and printing must not be permitted from the XXXX hosted system within the BDS. Any additional applications or tools installed must not introduce security weaknesses |
| XXXX Dedicated Space | System and Desktops | Patching and updating processes and procedures must be in place to cover automatic and manual patching |
| XXXX Dedicated Space | Testing and development environment | Software development must only be performed for XXXX owned programs within the BDS |
| XXXX Dedicated Space | Source Code | Source code must be securely executed, stored and sent to XXXX. |

|  |  |  |
| --- | --- | --- |
| XXXX Dedicated Space | Network Controls - Transmission | All the information must be transmitted securely between BDS environment and XXXX and the management of network devices must be done using secure protocols |
| XXXX Dedicated Space | Network Controls - Routing | Routing configuration must ensure only connections to the XXXX network and must not route to any other networks |
| XXXX Dedicated Space | Network Controls - Wireless | Wireless networks must not be used in the XXXX network segment to provision services. |
| XXXX Dedicated Space | Network Segregation | There must be separate network segments (i.e. business processing / live system support / systems development) |
| XXXX Dedicated Space | File Storage | All file storage must be within BDS environment |

|  |  |  |
| --- | --- | --- |
| XXXX Dedicated Space | Network Segregation | There must be separate network segments (i.e. business processing / live system support / systems development) |
| XXXX Dedicated Space | File Storage | All file storage must be within BDS environment |

# Cryptography– Minimum Control Requirements

|  |  |  |
| --- | --- | --- |
| **Control Area** | **Control Title** | **Control Description** |
| Cryptography | Cryptographic Key Management | For Projects/Suppliers where secret or private cryptographic keys are used to protect XXXX Data identity and/or reputation, the keys are managed securely throughout their lifetime, in accordance with documented control requirements and procedures which are consistent with XXXX-POL-ALL-016 - Encryption & Key Management Policy, and shall ensure that the keys are protected against unauthourised access or destruction. |
| Cryptography | Cryptographic Key Management | The XXXX shall maintain a record of all cryptographic use, including all keys, certificates and cryptographic devices |
| Cryptography | Public Key Infrastructure | The XXXX shall ensure that if public key infrastructure (PKI) is used or operated, it shall be protected  by ‘hardening’ the underlying operating system(s) and restricting access to Certification Authorities. |

|  |  |  |
| --- | --- | --- |
| Cryptography | Public Key Infrastructure | The XXXX shall ensure that all digital certificates that represent XXXX are centrally managed to ensure the certificate continued validity. |

# Procedure Compliance & Enforcement

## Compliance Measures

Not applicable.

## Enforcement

All staff of XXXX must comply with all Information Security Procedures. Failure to comply with these procedures 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.

# Glossary / Acronyms

## Glossary / Acronyms

|  |  |
| --- | --- |
| HSM | Hardware Security Module |
| FIPS | Federal Information Processing Standards |
| BDS | XXXX Dedicated Space |

# Document Management

## Document Revision Log

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

## Document Ownership

This Procedure is owned by the YYYY

## Document Coordinator

This Procedure is coordinated by the YYYY

## Document Approvers

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

## Distribution

* *Distribution is to all staff*