VENDOR MANAGEMENT & DUE DILIGENCE POLICY

*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 3

1.1 Document Definition 3

1.2 Objective 3

1.3 Scope 3

1.3.1 Applicability to Employees 3

1.3.1 Applicability to External Parties 3

1.4 Related Documents / References 3

2. Policy Statements 4

2.1 Policy and Standard Compliance 4

2.2 Third-Party Selection 4

2.3 Establishing Contracts 4

2.4 Risk Assessment 4

2.5 Right to Audit 4

2.6 Encryption 4

2.7 Granting Limited Access 5

2.8 Issue / Breach Notification 5

2.9 Vendor Compliance and SLA Review 5

2.10 Approved Vendor List 5

2.11 Termination and Removal 5

2.12 Responsibility for Vendor Coordination & Oversight 5

3. Policy Compliance & Enforcement 6

3.1 Compliance Measures 6

3.2 Enforcement 7

4. Exception Process / Glossary 8

4.1 Exception Process 8

4.2 Glossary / Acronyms 8

5. Document Management 9

5.1 Document Revision Log 9

5.2 Document Ownership 9

5.3 Document Coordinator 9

5.4 Document Approvers 9

5.5 Document Distribution 9

# Introduction

## Document Definition

This document is a Policy.

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

## Objective

The purpose of this policy is to set forth rules governing security and due diligence requirements for Third Party Vendors and Business Partners doing business with XXXX. (XXXX).

This policy applies throughout the third-party lifecycle from the beginning of the vendor selection process, through utilisation and termination of the relationship.

## Scope

### Applicability to Employees

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

### Applicability to External Parties

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

## Related Documents / References

* *XXXX-POL-ALL-001 - Information Security Policy Framework*
* *XXXX-POL-ALL-004- Data Classification Policy*
* *Risk Management Policy*
* *XXXX-POL-ALL-016- Cryptography & Key Management Policy*
* *XXXX-PRC-ALL-016- Vendor Due Diligence Procedure*

# Policy Statements

## Policy and Standard Compliance

All external vendors must comply with XXXX Information Security Policies and Standards applicable to the service being provided. XXXX Policies and Standards must be provided to external vendors when required.

## Third-Party Selection

The effectiveness of information security practices and standards of potential external vendors must be taken into consideration during the selection process.

See *XXXX-PRC-ALL-016 - Vendor Due Diligence Procedure.*

## Establishing Contracts

Documented agreements, such as contracts or service level agreements must be established with all external vendors and must be reviewed by the legal department prior to execution. Agreements must also comply with all applicable laws and regulations.

Agreements must include all security requirements and insurance needs where applicable.

## Risk Assessment

In accordance with the *Risk Management Policy*, a risk assessment must be conducted on the information security controls of the proposed sharing of information prior to the execution of a contractual agreement. This assessment may be performed as part of a standard vendor assessment process.

## Right to Audit

Contractual agreements must specify the right to audit work carried out by external vendors, provide details of licensing arrangements, and define the ownership of intellectual property rights. Where appropriate, external vendors must furnish XXXX with independent audit reports (e.g., SSAE-16, Type II) outlining their control environments that support XXXX information assets.

## Encryption

All XXXX information exchanged with external vendors must be encrypted in transit. If the information is defined by the *XXXX-POL-ALL-004- Data Classification Policy* as RESRICTED or CONFIDENTIAL, the information must be encrypted at rest and comply with *XXXX-POL-ALL-016- Encryption & Key Management Policy*.

## Granting Limited Access

Access to XXXX network, applications, and information must be explicitly granted by XXXX to external vendors only when it is linked to a specific documented responsibility. Access must be limited to only those information assets required to fulfil the responsibility, for time required to complete a specific task, and be monitored while active.

## Issue / Breach Notification

External vendors must notify XXXX management of any known or suspected problems related to the control of XXXX information assets or systems in a timely manner.

## Vendor Compliance and SLA Review

If applicable, the regulatory compliance status and/or Service Level Agreement (SLA) conformity must be reviewed on an annual basis.

## Approved Vendor List

All vendors providing services to XXXX will be centrally recorded.

## Termination and Removal

Upon termination of an external vendor relationship, the following actions must be performed in a timely manner as dictated by the terms of the contractual agreement:

* All information sharing connections and/or mechanisms must be disabled and removed;
* All individual information and network access must be disabled and removed;

XXXX information assets must be returned in a usable format and permanently removed and/or destroyed by the external vendor.

## Responsibility for Vendor Coordination & Oversight

Individual responsibility for the coordination and oversight of all XXXX third-party vendor relationships must be assigned and recorded.

Management of the vendor list is the responsibility of the IT and General Services department.

# Policy Compliance & Enforcement

## Compliance Measures

If applicable, compliance with the above Policy can be measured by the following criteria. Example evidence will vary depending on any supporting guidelines implemented to support this Policy. 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 external vendor agreements, evidence that appropriate due diligence was performed during the contracting process, for example:   * The third party is contractually required to comply with XXXX security policies and standards * The external vendor’s security controls were considered during the selection process * Agreements were reviewed by the legal department * A Risk Assessment was performed in accordance with the Risk Assessment Policy * A “Right to Audit” clause was specified in the agreement and/or a SSAE-16, Type II or similar independent audit report was provided * The standard vendor assessment was completed | * Documented due diligence review report * Contract document * Security assessment report of independent third-party * Sign-off (physical or electronic) by the legal department * Completed standard vendor assessment |
| For a selection of data classified as Restricted or Confidential that is shared with external vendor, evidence that the data is encrypted when transferred between XXXX and the external vendor | * Network configuration information * Sample data packet analysis |
| For a selection of access granted to external vendors, evidence that the access is restricted to only the required information for the external vendors to perform their responsibilities | * System and/or network configuration information * User Access request forms/mails |
| For a selection of issue notifications received from external vendors, evidence that notice was received in a timely manner | * Email notifications * Hard copy letters / faxes |
| For a selection of terminated external vendor connections, evidence of the timely termination of the agreement and supporting network connections | * Email notifications * Hard copy letters / faxes * Network configuration information |

## Enforcement

All staff of XXXX must comply with all Information Security Policies. Failure to comply with these policies 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 Policy 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

|  |  |
| --- | --- |
| SLA | Service Level Agreement |

# Document Management

## Document Revision Log

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

## Document Ownership

This Policy is owned by the YYYY

## Document Coordinator

This Policy is coordinated by the YYYY

## Document Approvers

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

## Document Distribution

The Document Owner controls distribution of this document. The distribution is as follows:

* All Staff