VENDOR DUE DILIGENCE 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 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

1.3.2 Applicability to Assets 3

1.4 Related Documents / References 3

2. Standard Statements 4

2.1 Minimum Process 4

2.2 Minimum Background Information 4

2.3 Contract Prerequisites 4

2.4 Security Prerequisites 4

2.5 Identification of Risks Related to External Parties 5

2.6 Addressing Security in External Party Agreements 6

2.7 Independent Review 6

3. Standard Compliance & Enforcement 7

3.1 Compliance Measures 7

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 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 global information security requirements for the choosing, engagement, and onboarding of third-party vendors and outsourcers.

## 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-PRC-ALL-016 – Supplier Due Diligence Assessment Procedure*

# Standard Statements

## Minimum Process

At a minimum, service and outsourcing service contracts must be developed according to the following process:

1. assess the business need and cost/benefit analysis;
2. prepare a Request for Proposal (RFP);
3. evaluate vendors;
4. identify contract requirements; and
5. monitor outsourced activities.

## Minimum Background Information

The Executive Committee (EC)/ Security Committee (SC) must before approval request background information for new or unknown vendors that may include:

* control structure;
* security requirements;
* financial statements;
* customer referrals;
* coverage for sub-contracting;
* bank guarantee;

## Contract Prerequisites

At a minimum, all outsourcing contracts must contain:

* designation of property/asset ownership;
* actions related to violations;
* conditions for access to XXXX locations and assets;
* a Right to Audit;
* Service Level Agreements (SLA) where necessary;

## Security Prerequisites

At a minimum, all outsourcing contracts must contain:

* agreements on acceptable security controls and policies;
* determination of acceptable service levels and availability;
* documentation of physical and logical controls employed by outsourcer to protect the confidentiality, integrity, and availability of XXXX assets;
* determination of all legal and regulatory requirements including those for privacy and data protection;
* agreement that outsourcer must test and maintain system security on an on-going basis;
* breach notification including unauthorised access to, or compromise of, data or resources.

## Identification of Risks Related to External Parties

1. External parties shall only be granted access to the XXXX’s information resources and processing facilities where a clear business need for such is established, with the explicit approval of the data/system owners, and only with the minimum access needed to accomplish the business objective.
2. These external parties include but are not limited to:
3. Service providers;
4. Managed security services;
5. Outsource service suppliers (facilities maintenance, operations management, systems administration, data collection, call-centre operations etc.);
6. Consultants, Auditors and Regulators;
7. Systems developers and suppliers of IT systems and services;
8. Cleaning, catering and other outsourced support services;
9. All external parties granted access to any of the XXXX’s information resources shall be subject to the relevant provisions of the XXXX’s Information Security Policies.
10. All the respective relationship owners responsible for services in any of the above listed categories are required to liaise with the Legal Department to ensure that the external parties concerned have executed a formal contract agreement incorporating the applicable terms and conditions for accessing the XXXX’s information resources and systems.
11. Relationship owners are responsible for ensuring that the security controls, service definitions and delivery levels included in external party agreements are implemented, maintained and operated by the external party.
12. The XXXX shall agree with the external party those controls that the external party is required to implement and document them in the agreement (drawn up or reviewed by the Legal Department) that shall be executed by both parties. The external party shall be required to ensure that all its personnel are aware of their obligations under the contract.

## Addressing Security in External Party Agreements

1. Agreements with external parties involving accessing, processing, communicating or managing the XXXX’s information or information processing facilities, or adding products or services to information processing facilities shall cover all applicable security requirements.
2. The contract agreements between the XXXX and external parties for such services shall be created and/or reviewed by the XXXX’s Legal Department in consultation with the service owner’s department and IT/Information Security department.
3. Where an external provider has a standard agreement and no provision to vary it to meet a client’s requirement, the external party’s standard clauses shall be assessed against the XXXX’s requirements and the risk associated with any noted gaps shall be assessed before deciding whether or not to proceed with the offered terms. Where there is a significant variation between the XXXX’s requirements and what is offered, the Chief Risk Officer’s approval to proceed with the provider must be obtained.
4. All major suppliers are evaluated on an annual basis.
5. The SLA’s with business-critical suppliers are fully reviewed. Where practical an audit or evaluation report may be sought from these suppliers to the effectiveness of their Information Security Management System (or equivalent).

The minimum-security requirements must follow the *XXXX-PRC-ALL-016 – Supplier Due Diligence Assessment Procedure*

## Independent Review

Depending on the sensitivity and criticality of the services or data provided, XXXX may consider commissioning or requesting an independent review of the service provider’s internal control and information security structure.

# 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 sample of suppliers check if information security was addressed | * Review sample SLAs and NDAs |
| For a sample of vendors check if proper approval is in place | * Review security committee minutes and vendor approval list |

## 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

|  |  |
| --- | --- |
| SLA | Service Level Agreement |
| NDA | 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** |
|  |  |  |

## Document Distribution

Distribution is to all staff