Legal, Regulatory and Contractual Requirements Procedure

*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

1.3.1 Applicability to Assets 3

1.4 Related Documents / References 3

2. Legal, Regulatory and Contractual Requirements Procedure 4

2.1 Identify Requirement 5

2.2 Assess Implications 6

2.3 Document Requirements 6

2.4 Define Approach to Meeting Requirements 6

2.5 Review and Update 6

3. Procedure Compliance & Enforcement 7

3.1 Compliance Measures 7

3.2 Enforcement 7

4. Glossary / Acronyms 8

4.1 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 Distribution 9

# 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

In creating and maintaining an ISMS it is vital that a full understanding is gained of the various legal, regulatory and contractual requirements that apply to **Error! Unknown document property name.** and its business. This will ensure that the XXXX continues to meet its obligations and its board of directors and other stakeholders are not exposed to the risk of criminal prosecution or corporate liability.

The purpose of this procedure is to document how such requirements are identified and incorporated into the ISMS and how updates to the requirements are handled.

## 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*
* *Information Security Context, Requirements and Scope*

# Legal, Regulatory and Contractual Requirements Procedure

The procedure for identifying, documenting and maintaining legal, regulatory and contractual requirements is summarised in the diagram below. Each step is expanded upon in the following sections.



## Identify Requirement

XXXX relies upon the following internal teams and external bodies to identify legal, regulatory and contractual requirements that are relevant to its information security:

|  |  |  |
| --- | --- | --- |
| **Team/organization** | **Areas Covered** | **Method of Communication** |
| Legal department | Laws relevant to information security, including privacy and data protection | Email alerts  Quarterly meetings |
| External legal advisers | Laws relevant to information security, including privacy and data protection | Webinars  Newsletters  Meetings on specific topics |
| Governance, Risk and Compliance team | Regulatory framework and requirements  Regulatory reporting | Email alerts  Quarterly meetings |
| Supplier Management | Contractual agreements, current and new bids | Email alerts  Quarterly meetings |
| Industry body | Laws, regulations and other issues relevant to our industry | Seminars  Annual Conference |
| Regulatory Authority | Regulatory framework and requirements  Regulatory reporting | Official communications  Briefing events |
| Professional associations for information security | General legal, regulatory and contractual issues for information security | National and regional meetings  Newsletters  Training |
| National and regional business groups | General legal, regulatory and contractual issues for the business | National and regional meetings  Newsletters  Training |

In general, XXXX will rely upon the appropriate team or external body to provide an interpretation of the relevant parts of the item under consideration. This may be in the form of briefing papers, presentation materials or other media.

Where necessary, the Legal Officer shall obtain full copies of the relevant source material (such as legislation or regulatory announcements) for reference purposes. These may be in hardcopy or electronic form.

## Assess Implications

The ISO/Legal Officer is responsible for ensuring that a full assessment of the implications of the relevant items for the ISMS is carried out. This will be based upon qualified advice from the relevant sources listed in the table above.

The assessment will include the following aspects:

* Degree of change to the ISMS and its associated policies, procedures, forms and plans needed to meet the requirement
* Urgency of meeting the requirement
* Consequences of not meeting the requirement
* Available options for meeting the requirement

## Document Requirements

Once assessed, the relevant requirements will be documented at a high level as part of the ISMS within the document *Information Security Context, Requirements and Scope*. All changes to this document will be recorded in accordance with the ISMS documentation procedures.

Details of the requirements will be documented in the *Legal, Regulatory and Contractual Requirements sheet*. These details will include:

* Name
* Source of the requirement
* Type of requirement – legislative, regulatory, contractual, other
* Details of the requirement, at an appropriate level
* Requirements of interested parties relevant to the ISMS
* Owner of the requirement
* Evidence of Compliance

Where needed, confirmation of the interpretation of the requirement will be obtained from a relevant source e.g. the organization legal department.

## Define Approach to Meeting Requirements

Where immediate changes are needed to the ISMS as a result of a new or changed requirement these will be incorporated as soon as possible, and revisions issued to all recipients of the relevant policies and procedures. Otherwise the change will be considered at the next annual review of the ISMS.

## Review and Update

New requirements and changes to existing requirements will be discussed at regular review meetings with internal departments, particularly:

* Legal department
* Governance, Risk and Compliance team
* Security Committee
* Operations
* Human Resources

All relevant requirements will be re-assessed on at least an annual basis as part of the ISMS annual review. Appropriate advice will be obtained at this point to ensure that all changes have been captured.

Any new or changed requirements identified as part of the review process will be handled in accordance with this procedure and appropriate updates made.

# 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

|  |  |
| --- | --- |
| ISO | Information Security Officer |

# Document Management

## Document Revision Log

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

## 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

All Staff