COMMUNICATIONS 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 Policy Details 3

1.1 Internal Communications 3

1.2 External Communications 4

2. Policy Compliance & Enforcement 5

2.1 Compliance Measures 5

2.2 Enforcement 5

3. Exception Process / Glossary 5

3.1 Exception Process 5

3.2 Glossary / Acronyms 5

4. Document Management 5

4.1 Document Revision Log 5

4.2 Document Ownership 6

4.3 Document Coordinator 6

4.4 Document Approvers 6

4.5 Document Distribution 6

# 

# Introduction

This policy describes the modes of communication of Information Security for XXXX to ensure confidentiality, integrity and availability of information assets are maintained and satisfy and comply with the requirements of the ISO 27001:2013 Standard. It outlines communication lines with key inputs and outputs of the Information Security Management System communication

The following policies and procedures are relevant to this document:

XXXX-POL--ALL-002 - Acceptable Use Policy

XXXX-POL--ALL-004 - Data Classification Policy

# Policy Details

## Internal Communications

All ISO related and Information Security matters should be communicated using the following methods detailed in the table below:

* Roles: Who is responsible for communicating
* What: Outputs that are to be communicated
* When: Frequency of communication
* Who: Intended audience for the communication
* Method: How information is communicated

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Roles | What | When | Who | Method |
| Top Management | Objectives | Annually | All Staff | Policy Statement |
| Management Review | Annually | Security Committee | Management Review Minutes |
| Security Committee (SC) | Management Review | Quarterly | Top Management | Management Review Minutes |
| Head IT/CISO | All Information Security matters | Ongoing Basis | Top Management /  SC | Email  Phone  Verbal  Reports |
| Management Representatives | Action and Treatment Plans | Bi-annually | SC | Reports |
| External Audits | Annually | SC | Reports |
| Risk Assessments | Annually | SC | Reports |
| Internal Audits | Annually | Certification Body/  SC | Reports |
| Policies | Annually/Upon request | All Staff/  Certification Body/  Designated Interested Parties | Intranet  Email  Banners |
| Processes | Annually/Upon request | All Staff/  Certification Body/  Designated Interested Parties | Intranet |
| Business Continuity Plans (BCP) | Annually/Upon Changes | BCP Teams | Emails  Meetings |
| Information Security Internal Auditors | Information Security Audit Plan | Annually | Management Reps | Information Security Audit Plan |
| Information Security Audit Results | Annually | Management Reps | Information Security Internal Audit Reports |
| All Employees | Incidents | Ongoing | Head of Department/  Incident Response Team | Email  Memos  Helpdesk |
| Events | Ongoing | Head of Department/  Incident Response Team | Email  Helpdesk |
| Non-conformances | Ongoing | Head of Department/  Incident Response Team | Email  Helpdesk |
| Improvements | Ongoing | Head of Department/  Management Reps | Email  Meetings |

## External Communications

* All ISO documentation are classified as per the Information Classification Policy.
* Only documents that are classified as Public Information may be distributed to designated interested parties.
* Should any interested party request access to other classifications of documents they are to be invited to premises and supervised whilst viewing these documents.
* No copies are allowed to be transferred to external parties. Alternatively, redacted and therefore declassified versions of documents may be distributed to external parties.

# 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** |
| * Ensure intended personnel get communications on ISO 27001 awareness, progress, updates, results and performance | * Check mails, memos, banners and documents received in communication of ISO 27001 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

|  |  |
| --- | --- |
| ISO | International Standards Organisation |
| SC | Security Committee |

# 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

* All Staff