ACCEPTABLE USE POLICY

*Revision: r1.0*

*Effective Date: dd-mm-yyyy*

*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. Policy Statements 4

2.1 Acknowledgement of User Responsibilities 4

2.2 Assets and Intellectual Property 4

2.3 Monitoring 4

2.4 Access to Data 4

2.5 Moving, Copying, and/or Storage of Data Assets 4

2.6 Role and Function 4

2.7 Unacceptable Use 4

2.8 Installation of Software Packages 5

2.9 Network Wide Emails & Mass Mailing 6

2.9.1 Send to All 6

2.9.2 Mailing List, Address Book & Database Held Addresses 6

2.10 Personal Use 6

2.11 Disciplinary Process for Data Breaches 6

2.12 Continuation of Responsibility 7

3. Policy Compliance & Enforcement 8

3.1 Compliance Measures 8

3.2 Enforcement 8

4. Exception Process / Glossary 9

4.1 Exception Process 9

4.2 Glossary / Acronyms 9

5. Document Management 10

5.1 Document Revision Log 10

5.2 Document Ownership 10

5.3 Document Coordinator 10

5.4 Document Approvers 10

5.5 Document Distribution 10

# 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 objective of this policy is to outline the acceptable use of electronic and data assets at XXXX (XXXX). Inappropriate use exposes XXXX to risks including, compromise of network systems, services and data, negative commercial impact, and People / Legal issues.

Assets may include but are not limited to:

* Electronic Media;
* Desktop and Laptop Computers;
* Servers;
* Network Infrastructure;
* Telephones;
* Mobile Computing and Communication Devices

## 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.

### Applicability to Assets

This Policy 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-POL-ALL-025 - Information Disposal Policy*
* *XXXX-POL-ALL-005 Data Handling & Retention Policy*
* *XXXX-POL-ALL-003 - Acceptable Use Policy – End User Agreement*

# Policy Statements

## Acknowledgement of User Responsibilities

All users must review and acknowledge their understanding of the *XXXX-POL-ALL-002 - Acceptable Use Policy* (this policy) and other related information security policies on an annual basis.

## Assets and Intellectual Property

All information systems assets provided by XXXX remain the sole property of XXXX. Any data or intellectual property created by the user remains the property of XXXX and should not be removed, copied or shared with any person or entity except as part of the user’s normal job responsibilities.

Intellectual Property includes, but is not limited to; patents, copyrights, trademarks, and material such as; strategic plans, products, computer programs etc.

## Monitoring

Where allowed by law, XXXX reserves the right to monitor all activities that occur on its electronic assets, whether on XXXX owned or leased systems, or on any other permitted devices used for XXXX work purposes.

## Access to Data

Where allowed by law, XXXX reserves the right to access any data that resides on its electronic assets, whether on XXXX owned or leased systems, or on other permitted devices containing XXXX data assets.

## Moving, Copying, and/or Storage of Data Assets

Unless protected by security controls at least equal to those enforced internal systems, and explicitly approved by the relevant Data Owners, it is prohibited to move, copy, or store data above classification level INTERNAL on local hard-drives, or removable electronic media.

* Further, all information assets will be protected (at a minimum) to any applicable Industry Standard or Regulation as defined in the *XXXX-POL-ALL-005 Data Handling & Retention Policy*

## Role and Function

Use of XXXX electronic assets must be consistent with the individual’s role within the organisation and intended function of the asset.

## Unacceptable Use

Using XXXX electronic assets for abusive, unethical, or inappropriate purposes will not be tolerated and may be considered grounds for disciplinary action, including termination of employment for gross misconduct and potentially legal action.

Unacceptable use of electronic assets includes, but is not limited to:

* the transmission of any XXXX data above INTERNAL unencrypted over end user messaging technologies, including - but not limited to – email, instant messenger, SMS, text etc;
* deliberately accessing, creating or transmitting any obscene or indecent images, data or other material, or any data capable of being resolved into obscene or indecent images or material;
* creating or transmitting material which is designed or likely to cause offence, annoyance, inconvenience or needless anxiety to another;
* creating or transmitting defamatory material or material that is libellous of any other person’s or company’s reputation, products or services;
* viewing, transmitting, copying, downloading or producing material, including (but not exhaustively) software, films, television programs, music, electronic documents and books which infringes the copyright of another person, or organisation;
* making offensive or derogatory remarks about staff or XXXX on interactive life-style websites (Social Media) such as Facebook, Twitter, YouTube etc.;
* posting offensive, obscene or derogatory photographs, images, commentary or soundtracks on interactive life-style websites (Social Media) such as Facebook, Twitter, YouTube etc.;
* any other act that contravenes the *XXXX-POL-ALL-003 - Acceptable Use Policy - End User Agreement*;
* transmitting or producing material which breaches confidentiality undertakings;
* attempting to gain deliberate access to facilities or services which the user is unauthorised to access;
* deliberately undertaking activities that corrupt or destroy other user’s data;
* disrupt the work of other users, or deny network resources to them;
* violate the privacy of other users;
* waste staff effort or networked resources;
* creating or transmitting unsolicited commercial or advertising material unless that material is part of a service to which recipients have chosen to subscribe;
* making commitments via email or the internet on behalf of XXXX without full authority;
* undertaking any activities detrimental to the reputation or business interests of XXXX;
* deliberately contributing to News Groups or web sites that advocate illegal activity;
* initiating or participating in the sending of chain letters, ‘junk mail’, ‘spamming’ or other similar mailings;
* Illegal activities;
* Revealing or publicising XXXX intellectual property or proprietary information for unapproved or non-business related reasons;
* Sharing of usernames and/or passwords;
* Presenting your own viewpoints or positions as those of XXXX, or attributing them to XXXX;
* Providing information about, or lists of, XXXX employees to external parties

## Installation of Software Packages

The installation of software packages not approved by Head of IT is strictly prohibited.

Requests for approval shall be processed through the *XXXX-POL-ALL-038 - Software Policy*.

Approved software list is maintained by the Head of IT.

## Network Wide Emails & Mass Mailing

### Send to All

The distribution of network-wide emails using the ‘All’ or ‘Reply to All’ (or equivalents) or by harvesting global address lists is prohibited unless sent by authorised personnel, or for welfare or urgent operational notifications that need to be brought to the attention of all staff.

Examples of messages deemed as being appropriate for widespread distribution include, but are not limited to, those concerning:

* security issues, such as bomb or terrorist threats and computer system viruses and other threats;
* health and safety matters such as hazard warnings and natural disaster alerts;
* urgent upgrades of the network services that may result in temporary disruption to systems;
* the announcement of XXXX Policies that are time critical or which staff have to be made aware of for legal compliance reasons;
* informing staff of new pay structures or industrial action;
* important announcements from the Board or Senior Management;
* press releases;
* time critical financial and administrative deadlines.
* Cyber security and information security awareness information

Network-wide emails should not be used to circulate messages or images of a personal nature, e.g. personal photographs, personal news, items for sale, etc.

### Mailing List, Address Book & Database Held Addresses

Employees who send emails to internal or external multiple recipients by compiling a list from a personal address book or database are to enter the email addresses in the Bcc: field or other mechanism so that they cannot be seen and harvested by others.

All removal requests are to be actioned by the recipient on receipt.

## Personal Use

Employees are expected to use common sense and exercise good judgment regarding the reasonableness of personal use of XXXX information systems assets, and when unsure, should contact their managers or human resources representatives for further information.

## Disciplinary Process for Data Breaches

A formal and communicated disciplinary process must be in place to take action against employees who have committed, or are egregiously responsible for, a breach of XXXX data or physical assets.

The process will follow these parameters at a minimum. The formal disciplinary process will:

* ensure correct and fair treatment for employees who are suspected of committing breaches of information security;
* provide for a graduated response that takes into consideration factors such as the nature and gravity of the breach and its impact on business, whether or not this is a first or repeat offence, whether or not the violator was properly trained, relevant legislation, business contracts and other factors as required, and;
* be used as a deterrent to prevent employees from violating XXXX’s information security policies and procedures.

## Continuation of Responsibility

Employment contracts, term and conditions of employment, and similar documents will contain sufficient clauses to ensure the ongoing maintenance of security responsibilities in the case of employment change or termination.

# 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** |
| Evidence of users review and acknowledgement of their understanding of XXXX Acceptable Use Policy and other related information security policies. | * New hire training user sign-off documentation * Electronic responses to periodic surveys or security awareness training |
| Evidence that users are complying with the concepts of acceptable use. | * Level of exceptions reviewed by management and audit on violations of acceptable use |

## 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

|  |  |
| --- | --- |
| XXXX | XXXXXX |
|  |  |

# Document Management

## Document Revision Log

|  |  |  |  |
| --- | --- | --- | --- |
| **Date** | **Editor** | **Revision #** | **Description of Change** |
| dd-mm-yyyy |  | r1.0 | Creation and approval of new policy |

## Document Ownership

This Policy is owned by the Executive Committee

## Document Coordinator

This Policy is coordinated by the Head IT

## Document Approvers

|  |  |  |
| --- | --- | --- |
| **Approver Name** | **Signature** | **Date** |
| Executive Committee |  | dd-mm-yyyy |
|  |  |  |

## Document Distribution

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

* All Staff
* Approved third parties and vendors