SOFTWARE 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

1.3.2 Applicability to Assets 3

1.4 Related Documents / References 3

2. Policy Statements 4

2.1 Purchasing Software 4

2.2 Software Licensing & Registration 4

2.3 Software Installation 4

2.4 Removal of Software 4

2.5 In-House Software Development 5

2.6 Modifications to Software Packages 5

2.7 Use of Software in a Cloud Environment 5

3. Policy Compliance & Enforcement 6

3.1 Compliance Measures 6

3.2 Enforcement 6

4. Exception Process / Glossary 7

4.1 Exception Process 7

4.2 Glossary / Acronyms 7

5. Document Management 8

5.1 Document Revision Log 8

5.2 Document Ownership 8

5.3 Document Coordinator 8

5.4 Document Approvers 8

5.5 Document Distribution 8

# 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

This policy sets out how software will be acquired, registered, and installed within XXXX

## 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-002 - Acceptable Use Policy*
* *XXXX-POL-ALL-011 - Risk Management Policy*
* *XXXX-POL-ALL-014 - Vulnerability Management Policy*
* *XXXX-POL-ALL-019 - Secure Software Development Policy*
* *XXXX-STD-ALL-021 - Software Development Life Cycle*
* *XXXX-PRC-ALL-002 - Change Management Procedure*

# Policy Statements

## Purchasing Software

All computer software to be used within the organization must be purchased through IT department or at least IT carried along in the procurement and installation process. This is necessary to ensure that:

* Licensing requirements are addressed
* The software works effectively with the standard corporate software image
* Use of the software can be supported by the IT department
* Best value for money is obtained in procurement
* A record is kept of installed software within the organization

## Software Licensing & Registration

All software in use within XXXX must be correctly licensed. This is a legal requirement and compliance is monitored by various industry bodies including FAST (Federation Against Software Theft).

All installed software programs will be registered in the name of the organization, not the individual. Purchased software is a corporate asset and licenses will frequently be reused as the shape of the organization changes.

Under no circumstances must corporate software be copied (other than for backups) or installed for use on non-corporate machines, such as at home.

The IT Department will maintain a register of all licensed software within the organization and licensed copies of media such as DVDs.

Asset management software will be used to keep track of all installed instances of software titles and regular audits will be carried out. Any user with unlicensed software installed will be asked to remove it; it is the responsibility of users to ensure that all the software on their computer equipment is licensed.

## Software Installation

Licensed software will be installed by the IT department or appropriate technical team or supplier upon request and once any required licenses have been purchased.

Software will not be installed prior to a valid license being ordered.

The user must not install any software that is licensed to them personally, whether or not it is free, shareware or commercial. This includes evaluation versions of software programs.

## Removal of Software

If a software program is no longer required the IT department must be informed. The software will then be removed from the device in question and where possible the license will be re-used elsewhere within the organization.

Users must not remove licensed software from their devices without informing the IT department as this potentially represents a waste of a corporate asset.

## In-House Software Development

XXXX develops its own software for purposes where a commercial package is not available or does not fulfil the identified requirements. In such cases a structured development method will be used to ensure that software is developed to organizational standards and is tested and implemented in a managed way.

In-house software development must follow the *XXXX-STD-ALL-021 - Software Development Life Cycle.*

Any alterations to in-house developed software will be requested through the change request process. This process is described in the document *XXXX-PRC-ALL-002 - Change Management Procedure*.

## Modifications to Software Packages

Changes to Commercial Off The Shelf (COTS) software packages will not be made unless absolutely necessary, in which case they will be strictly managed and controlled. Where possible and commercially viable, changes will be made by the software vendor and supplied as standard updates.

## Use of Software in a Cloud Environment

Any applicable cloud-specific licensing and security requirements must be identified prior to installing software within a cloud environment. This is particularly relevant in circumstances where the cloud service provision is elastic i.e. the processing capacity increases and decreases with demand.

# 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 only licensed software are used by the XXXX | * Check that organisations like FAST have not notified the XXXX of use of unlicensed software |
| Ensure all installed software are licensed to XXXX and not individuals | * Confirm from sample of installed software who the software is licensed to |
| Ensure a register of licensed software is maintained | * Check licensed software maintained by IT |
| Ensure user cannot install personal software on their systems | * Check the list of installed software and confirm all of it are licensed to the XXXX * Attempt a software installation on random user’s systems |

## 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 | XXXX |
|  |  |

# 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