**Software Policy**

**Security Classification: Restricted**

**Document Ref. ISMS18008**

**Version: 1.0**

**Draft 1**

**Document Author:**

**Document Owner:**

Revision History

|  |  |  |  |
| --- | --- | --- | --- |
| **Version** | **Date** | **Change Number** | **Summary of Changes** |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

**Document Review**

|  |
| --- |
| **Date of Next Scheduled Review** |
|  |

Distribution

|  |  |
| --- | --- |
| **Name** | **Title** |
|  |  |
|  |  |
|  |  |

Approval

|  |  |  |  |
| --- | --- | --- | --- |
| **Name** | **Position** | **Signature** | **Date** |
|  |  |  |  |

**Contents**

[1 Introduction 6](#_Toc380575317)

[1.1 Risks Addressed 6](#_Toc380575318)

[1.2 Scope 6](#_Toc380575319)

[1.3 Related Documents 6](#_Toc380575320)

[1.4 Purpose 6](#_Toc380575321)

[2 Software Policy 7](#_Toc380575322)

[2.1 Purchasing Software 7](#_Toc380575323)

[2.2 Software Registration 7](#_Toc380575324)

[2.3 Software Installation 8](#_Toc380575325)

[2.4 Removal of Software 8](#_Toc380575326)

[2.5 In-House Software Development 8](#_Toc380575327)

# Introduction

## Risks Addressed

This document describes a control that was identified in [ISMS06004 Information Security Risk Treatment Plan](file:///C:\Users\Umar%20Farouk\OneDrive\Documents\TMP\ISO%2027001%20Information%20security%20management%20systems\ISO-27001-2013-V5R1\06.%20Planning\ISMS06004%20Information%20Security%20Risk%20Treatment%20Plan.doc) to address the following risks:

|  |  |
| --- | --- |
| **Reference** | **Description of Risk** |
|  |  |
|  |  |
|  |  |

## Scope

This control applies to all systems, people and processes that constitute the Project Management Office (PMO) information systems, including management, employees, and other third parties who have access to PMO.

## Related Documents

The following policies and procedures are relevant to this document:

* [ISMS13001 AUP and Personal Commitment Statement](file:///C:\Users\Umar%20Farouk\OneDrive\Documents\TMP\ISO%2027001%20Information%20security%20management%20systems\ISO-27001-2013-V5R1\A7.%20Human%20resources%20security\ISMS13001%20AUP%20and%20Personal%20Commitment%20Statement.doc)
* [ISMS18004 Change Management Policy](file:///C:\Users\Umar%20Farouk\OneDrive\Documents\TMP\ISO%2027001%20Information%20security%20management%20systems\ISO-27001-2013-V5R1\A12.%20Operations%20security\ISMS18004%20Change%20Management%20Policy.doc)
* [ISMS18005 Change Management Process](file:///C:\Users\Umar%20Farouk\OneDrive\Documents\TMP\ISO%2027001%20Information%20security%20management%20systems\ISO-27001-2013-V5R1\A12.%20Operations%20security\ISMS18005%20Change%20Management%20Process.doc)

## Purpose

The PMO uses many types of computer software to perform its business operations and always relies upon the correct functioning and security of that software. It is imperative therefore that steps are taken to ensure that only approved software is used within the Office and that no classified information is put at risk.

This policy sets out how software will be developed, acquired, registered, and installed within the PMO.

# Software Policy

## Purchasing Software

All computer software to be used within the Office must be purchased through the Project Management Unit. 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 Cybersecurity unit.
* Best value for money is obtained in procurement
* A record is kept of installed software within the Service.

## Software Registration

All software in use within the PMO must be correctly licensed, this is a legal requirement.

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

Under no circumstances will corporate software be copied (other than for backups) or installed for use on non-corporate machines, such as at home. This is against the law.

The Cybersecurity Unit will maintain a register of all licensed software within the Service and licensed copies of media such as CDs and DVDs in a Definitive Media Library (DML). This register will include:

* Physical location
* Inventory number
* Supplier
* Software description
* Issue date
* Number of disks in set
* License key(s)
* Any other relevant information

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 Cybersecurity Unit 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 will 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 Cybersecurity Unit will be informed. The software will then be removed from the machine in question and where possible the license will be re-used elsewhere within the Service.

Users must not remove licensed software from their machines without informing the Cybersecurity Unit as this potentially represents a waste of a corporate asset.

## In-House Software Development

The PMO develops its own software for particular 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 standards and is tested and implemented in a managed way.

Alterations to in-house developed software such as the addition of fields or screen changes may be requested through the change request process. This process is described in documents [ISMS18004 Change Management Policy](file:///C:\Users\Umar%20Farouk\OneDrive\Documents\TMP\ISO%2027001%20Information%20security%20management%20systems\ISO-27001-2013-V5R1\A12.%20Operations%20security\ISMS18004%20Change%20Management%20Policy.doc) and [ISMS18005 Change Management Process](file:///C:\Users\Umar%20Farouk\OneDrive\Documents\TMP\ISO%2027001%20Information%20security%20management%20systems\ISO-27001-2013-V5R1\A12.%20Operations%20security\ISMS18005%20Change%20Management%20Process.doc).

Changes to in-house developed software must not be made without following the change management process.