# Software Application Assets Management Policy

## Objective and Scope

The objective of this document is to ensure software application assets are selected, approved, installed and restricted in accordance with security needs, to ensure systems integrity and prevent exploitation of technical vulnerabilities. Strict controls and limitations are imposed on the use of privileged utility programs. Configuration management processes are in place for maintaining computer systems, servers, and software in a desired, consistent state.

The scope of this document takes into consideration any vendor supplied software which requires monitoring and control to avoid weaknesses occurring over time and any unauthorised changes.

## Roles, Responsibilities and Authorities

The Operations Director or competent IT Team delegate takes ownership of the selection, installation and control of restrictions of software applications. This includes configuration management and the selection and managing an approved software application asset register (White List).

Where an exception or deviation from an expectation or plan occurs, the senior assigned role shall make the determination in terms of what is an acceptable change. The change management process may need to be enacted.

## Legal and Regulatory

| Title | Reference |
|---|---|
| Data Protection Act 2018 | https://www.legislation.gov.uk/ukpga/2018/12/contents |
| General Data Protection Regulation (GDPR) | https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/ |
| The Telecommunications (Lawful Business practice)(Interception of Communications) Regulations 2000 | www.hmso.gov.uk/si/si2000/20002699.htm |
| Computer Misuse Act1990 | www.hmso.gov.uk/acts/acts1990/Ukpga_19900018_en_1.htm |
| The Privacy and Electronic Communications (EC Directive) Regulations 2003 | www.hmso.gov.uk/si/si2003/20032426.htm |
| Criminal Law Act 1967 | https://www.legislation.gov.uk/ukpga/1967/58/introduction |
| The Freedom of Information Act 2000 | https://www.legislation.gov.uk/ukpga/2018/12/contents |
| Online Safety Act 2023 | https://www.legislation.gov.uk/ukpga/2023/50/contents/enacted |
| National Assistance Act 1948 | https://www.legislation.gov.uk/ukpga/Geo6/11-12/29/enacted |
| Modern Slavery Act 2015 | https://www.legislation.gov.uk/ukpga/2015/30/contents/enacted |
| The Copyright, Designs and Patents Act 1988 | https://copyrightservice.co.uk/ |

# Software Application Assets Management Policy

| ISO 27001/2 REFERENCES | ISO 27001: 2013 Clause ID | ISO 27002: 2013 Annex A ID | ISO 27001: 2022 Clause ID | ISO 27002: 2022 Control ID |
|---|---|---|---|---|
| Operations - Use of privileged utility programs | 8.1 | | | 8.18 |
| Operational software control - installation | | 12.5.1 | | 8.19 |
| Technical vulnerability management | | 12.6.1 | | 8.8 |
| Configuration management | | | | 8.9 |
| Information deletion | | | | 8.10 |
| Data masking | | | | 8.11 |
| Data leakage prevention | | | | 8.12 |
| Restrictions on software installations | | 12.6.2 | | 8.19 |
| Information systems audit controls | | 12.7.1 | | 8.34 |

## Related Information

- Approved Software Applications Register (White list)
- Asset Register
- Information Classification Policy
- Change management procedure
- Incident reporting Policy
- Preferred Supplier Register

## Policy

The Operations Director determines the selection and approval, installation and platform user interfaces taking into account the:

- platform integrity and capabilities to meet specified needs
- prevention and exploitation of potential technical vulnerabilities

# Software Application Assets Management Policy

## Selection of approved software platforms - Approved Software Applications Register

Operational software, applications and program libraries are subject to registration in the approved software application register before being installed or updated. This shall only occur using executable code and never development code or compilers.

The Approved Software Applications Register (White List) shall include:

- Application name / vendor supplier / version number
- Current status of deployment against systems and assets

## Installation and updating of software on operational systems

Any proposed new release shall be approved by the Operations Director and risk assessed to ensure business needs are maintained, vulnerabilities are considered and information security is not compromised.

Prior to any installation or updating:

1. Test for usability, security and effects on other operating systems already in place (flow on effect) plus satisfactory user experience.
2. Test methods, programs and outcomes shall be recorded and approved as acceptable by Operations Director prior to being given the go ahead.
3. Maintain a configuration control system via the approved software applications register to track change management.

Before changes are made, document the following contingencies:

4. A proposed rollback plan and audit logs.
5. A library of previous software application versions and associated methodologies for future reference.

## Use of privileged utility programs

Strict controls and limitations are imposed on the use of privileged utility programs. The Operations Director controls access privileges to a select few IT Administrators.

The actual use of such programs only occurs after a risk review of the need and circumstances is undertaken in concert with the Operations Director and backups and protections confirmed as current. Segregation of utility programs from application software is standard practice.

## Technical vulnerability management

The Operations Director sources information about technical vulnerabilities of information systems constantly including following appropriate IT user groups and keeping abreast of known or suspected software application vulnerabilities. A risk assessment of vulnerabilities may need to be undertaken against business risk and taking into account assets listed on the Asset Register and known risks associated with these assets.

The following technical vulnerability indicators are in place:

- Monitoring of technical vulnerabilities including event logs
- IT user group information sources - vulnerability reporting
- Penetration testing

Risk controls as a result of a risk assessment shall include:

# Software Application Assets Management Policy

1. Assigned roles and responsibilities for managing both vulnerabilities and the change management process to mitigate vulnerability risk including monitoring, asset tracking, patching programs.
2. An action plan including schedule and timelines from risk assessment to control of technical vulnerabilities through a documented change management process

## Patches as a vulnerability control mechanism

In the case of a patch as a vulnerability control, before installing the patch undertake a risk assessment to confirm patch legitimacy and effectiveness prospects.

Test a patch in a controlled environment before progressing to installation and where necessary consider alternative controls such as:

- removing services or capabilities related to the risk
- add additional controls to manage the patch such as a firewall
- implement monitoring controls and flag the remaining risks.

Where a patch usage risk remains with no opportunity for effective control, raise an Incident Report and communicate the report to Operations Director for investigation and corrective action.

## Restrictions on software installations

All personnel working in the company or having access to the company systems, whether as an employee or other role (e.g. vendor or subcontractor) shall be subject to access controls as defined by their position or contract. This includes, however is not limited to:

- Assets assigned to the individual - refer Asset Register
- Access to secure information as defined in the Information Classification Policy
- Access controls according to need to know basis - least privilege allowance

Installation of applications other than those specified in the Approved Software Applications Register by the approved roles is not allowed and considered a breach of security.

## Configuration management

Configuration Management is the process of maintaining systems, such as computer hardware and software, in a desired state and ensuring systems continuously perform in a manner consistent with expectations.

The Operations Director or nominated delegate shall define and manage acceptable configuration protocols based on:

- the level of secure configuration appropriate to risk security (consider advice from white listed suppliers)
- priority protection given to sites holding PII data
- control and traceability over all configuration changes (change management protocols)

Configuration protocols

- Limit personnel with privileged /administrator access rights (Operations Director) to approve
- Clean up - disable unnecessary functions
- Strict control over default authentications
- Use a time-out that enacts the log off process.

Manage and monitor

# Software Application Assets Management Policy

- Log all configuration activities - who l when l what l version control l asset reference
- Monitor change - verify settings l password strengths l activities l anomalies

Integrate configuration management with asset management where practical. 'Physical (Equipment) Asset Management Procedure.

## Information deletion - also refer 'Media Handling Policy'.

Information deletion or clearing is the process of eradicating data on media. Protocols are in place for information deletion when no longer required to prevent unnecessary exposure and to meet contract / legal requirements.

When not required for specific reasons information shall be disposed of securely after the content has been securely wiped.

Methodologies for disposal can include shredding or data erasure via use by another application within an organisation. Credible data collection and disposal organisations may be used at the discretion of the Operations Director. Refer to the preferred supplier register for approved suppliers.

In order to maintain an audit trail, the disposal of confidential items must be logged and the register updated accordingly.

## Data masking

Data masking is a method of creating a structurally similar but inauthentic version of data that can be protected from misuse or used for purposes such as software testing and user training. The purpose is to protect the actual data while having a functional substitute for occasions when the real data is not required.

Data masking is also used to protect data by limiting exposure of sensitive information including PII and business contract information.

- Data masking can include anonymisation (irreversible)) or pseudonymisation (using a pseudonym and is reversible).
- Encryption can be used but requires a key to encrypt if legally requested to do so
- Deletion of information can be used to limit some exposure to data content
- Obfuscation of data is effective for health records (limits access without deletion)

Before any masking takes place review the legal and regulatory implications to ensure permanent, total deletion is legal.

## Data leakage prevention

## Information systems audit considerations

Any audit activity undertaken must be done in a manner that does not pose a risk to live operations and is a planned activity involving both management and the tester/auditor.

Prevision Research's operational systems shall be siloed from any audit activity. When undertaking audits, an audit plan shall be developed and agreed between all interested parties including:

- Agreement on scope of any technical audit activity

# Software Application Assets Management Policy

- Unless agreed and approved by the Operations Director that the audit cannot be done satisfactorily with read only access, supervised protections for sampled live access may occur (this is a high risk and should be avoided)
- Schedule audits outside normal business or main operating hours
- The audit process shall be monitored and logged for audit trail purposes

## Policy review

This policy shall be reviewed by the policy owner annually or immediately after a process change or a policy breach is known to have occurred. Refer below for the most recent review.

## History table

| Date | Rev No | Changes | Reviewed By | Approved By | Training Y/N |
|---|---|---|---|---|---|
| | | | | | |
| | | | | | |