**IT Hardware or Software**

**Acquisition Policy**

# Template

This is an example policy. Please ensure you update this policy template so that it’s suitable for your organisation.

## Policy statements

When developing, acquiring, or making major changes to an information system we will:

* prepare a ‘Statement of Sensitivity’ to determine the confidentiality, integrity, and availability requirements of the system
* apply security controls based on a ‘Threat and Risk Assessment’
* document the role and responsibilities related to information system security management.
* document specific procedures and standards used to mitigate risks and safeguard the information systems
* document and communicate procedures for security-related events and incidents

### Security requirements of information systems

1. Information security requirements must be considered in the acquisition of new information systems or enhancements to existing ones.
2. Identification and management of information security requirements and associated processes should be integrated into the early stages of information systems involving:
* acquisition
* upgrade
* repurposing and removal or disposal projects
1. Information security requirements and controls should reflect the business value of the information involved. This includes the potential negative business impact that might result from a lack of adequate security.

### Security application services on public networks

Before implementing an information system that involves electronic commerce on a public network, we must ensure its protection from:

* fraudulent activity
* contract dispute
* unauthorised disclosure
* modification

This is achieved by:

* conducting an information security requirements analysis (as mentioned in the previous section)
* ensuring that staff notification and acceptance of terms and conditions of use comply with policies and standards
* ensuring that multi-factor authentication (MFA) is used where applicable and based on data classification

### Protecting application services transactions

Information systems that involve online transactions must have security controls equal to the value and level of sensitivity of the information. We must ensure that security controls are implemented to prevent:

* incomplete transmission
* misrouting
* repudiation of a transaction
* unauthorised message duplication and replay

The following security controls will also be considered:

* validation and verification of user credentials
* digital signatures and encryption
* secure communication protocols
* storing online transaction details on servers within the appropriate network security zone

### Change control processes for information systems

We will ensure information security is included within the policies applying to software acquisition, development and systems.

Appropriate change control processes for systems are in place throughout the development lifecycle. This is coupled with technical reviews of applications for any changes made after operating platform changes.

Any changes to software packages should be minimised to only necessary changes, and those changes must be controlled.

Secure system engineering principles and development environment must be established. Any outsourced development must be strictly controlled and monitored.

### Restrictions on changes to software packages

A software update management process must be maintained for commercial off-the-shelf (COTS) software. This is intended to ensure the following:

1. Up-to-date and approved patches have been applied.
2. The version of the software in use is supported by the vendor.

Other than patches supplied by the vendor, COTS software must not be modified, except in extraordinary circumstances. For example, when needed for a critical business requirement. Those circumstances must be documented and approved by the information owner.

If changes to COTS software are required, the information owner and service owners must determine and document:

* the impact on security controls in the software
* the consent of the vendor (if required)
* that the functionality is included in a newer version of the software (if required)
* whether the organisation will be responsible for maintenance of the software after the change
* compatibility with other software in use

If changes are made to COTS software, the original version must be kept unaltered. The changes must be:

* logged and documented – including a detailed technical description
* applied to a copy of the original software
* tested and reviewed to ensure that the modified software operates as intended

## Exceptions

Exceptions to the guiding principles in this policy must be documented and formally approved by the <role> and <organisation>.

Policy exceptions must describe:

* the nature of the exception
* a reasonable explanation for why the policy exception is required
* any risks created by the policy exception
* evidence of approval by all appropriate parties

Review of this document: annually by the <role>.

Next review date: <date month year>.