**Acquisition of New Software or Hardware Policy**

**Template**

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

# Introduction

The <role> is responsible for overseeing all hardware and software acquisitions, and for maintaining all hardware and software products deployed within the <organisation>.

This policy is intended to define the process that hardware and software products are reviewed, purchased and maintained. This is in relation to data security, operational integrity and long-term sustainability.

<Organisation> will not install or support hardware and software that has not been approved in advance of purchase.

# Hardware

Computer hardware that connects to the network includes, but is not limited to:

* servers
* storage arrays
* routers
* switches
* wireless access points
* desktop computers
* laptop/notebook computers
* tablets
* printers
* security cameras
* VoIP (Voice over Internet Protocol) endpoints
* access controls
* UPS’ (uninterruptible power supply/source) and other computing and peripheral devices

# Software

A standard list of software applications for all new computers shall be:

* identified
* acquired
* installed
* configured

This approach should create a consistent technology environment that’s:

* secure
* compliant with all licensing and usage agreements
* meets the general requirements of <organisation>‘s ‘IT Security Policy’

# Process

Prior to procuring any hardware or software, the following must be adhered to.

## Software and vendor services review

1. <Organisation> will ensure that the hardware and or software meets all operational requirements. This includes:

* device configurations
* operating systems
* auxiliary or third-party software products (browser compliance, Java version)
* the user’s needs

1. In addition to the hardware and or software, <organisation> will also review data hosting and/or storage services. This includes data that’s hosted internally or by a third-party (a cloud agent acting on behalf of the vendor).
2. <Organisation> will assess the level of internal support necessary for continuous operation. The support services that are either provided by or will need to be purchased from the vendor.

## Vendor compliance

1. All vendors that provide hosting services must meet acceptable industry security standards, as well as specified <organisation> audit standards.
2. Vendors must provide evidence of their:

* SOC 1 or SOC 2 (Service Organisation Control) reports
* SSAE-16 (Statement on Standards for Attestation Engagements), formerly SAS-70, or comparable compliance documents
* audit reports (as needed)

This illustrates the vendor has committed an appropriate level of resources to data protection and security.

1. The software under review must provide a high-quality service that improves the <organisation>’s technology environment without risking:

* network or server performance
* data integration
* data security

1. All software that requires data exchange may include protected information. Therefore, it must comply with all UK legal and regulatory requirements.

## Hardware and Software demonstrations

1. All stakeholders must be included in vendor hardware and software demonstrations. <Organisation> recommends comprehensive demonstrations before the purchase of any software, and will work with vendors to arrange remote (WebEx) demonstrations, as needed.
2. In cases where institutional data may be required for demonstration purposes, vendors must provide, in advance, all security compliance documentation as specified above. This includes written assurance that all data will be permanently removed from their systems following the demonstration.
3. All relevant UK laws and regulatory requirements apply to hardware and software demonstrations.

## Budget

When purchasing new hardware or software, the budget must include the cost of the product as well as all associated costs. This includes:

* installation
* training services
* updates/upgrades
* third-party products that may be necessary for software operations
* costs associated with data transfers
* the cost of any specialized hardware or equipment that must be

An estimated cost of the annual maintenance and licensing fees must also be included. These costs should be planned and submitted across a 3 to 5 year period to include any planned version or release projections.

<Organisation> will assist with identifying all costs associated with the development of the budget. The requesting agency is responsible for identifying and securing budgetary funds for the acquisition, support and continuing costs of the:

* hardware
* software
* licensing
* maintenance

# Policy Compliance

## Compliance Measure

The <role> will verify compliance with this policy through various methods. This includes, but is not limited to:

* periodic reviews and site inspections
* video monitoring
* business tool reports
* internal and external audits and inspections
* feedback from those that procured the product

## Exceptions

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

## Non-compliance

Any agency found to have violated this policy may be subject to significant delays in the procurement process, as well as any future IT purchases.

The non-compliance situations may be subject to being published in <organisation>’s annual report to the legislature at the discretion of the <role>.

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

Next review date: <date month year>.