**APPENDIX D**

PSPS

Public Sector Partnership Services Ltd

# Information Security Policy System Acquisition, Development & Deployment

May 2024

# 1. Document Control

## Version Control

| Issue Number | Issue Author | Issue Date | Reason for Issue |
|---|---|---|---|
| **0.1** | J Wright | Mar 18 | Initial Draft for review |
| **1.0** | J Wright | Sept 18 | Revised in readiness for approval |
| **1.1** | J Wright | Feb 19 | Rebranded |
| **2.0** | J Wright | Feb 21 | Periodic policy review |
| **2.1** | J Wright | May 21 | Review to include Boston Borough Council |
| **2.2** | J Wright | Jan 22 | Additional of NCSC Cloud Security Principles |
| **3.0** | J Wright | May 24 | Periodic policy review & rebrand |

## Approval Control

| Issue Number | Approval Authority | Names | Approval Date | Due for Review |
|---|---|---|---|---|
| **3.0** | SHDC/ELDC/BBC | James Gilbert | May 24 | May 27 |
| | PSPS | Lewis Ducket | May 24 | May 27 |

## Policy Governance

| | |
|---|---|
| **Responsible** | Head of ICT & Digital |
| **Accountable** | Chief Executive (PSPS), Assistant Director (ELDC/BBC/SHDC) |
| **Consulted** | Data Protection Officers, ICT Security Lead |
| **Informed** | All ICT Users |

# Contents

# 2. Policy Overview

## Policy Aim

2.1 The aim of this Policy is to define the broad mechanisms and roles through which the Organisation will be able to demonstrate accountability and compliance with regards to Systems Acquisition, Development and Maintenance.

## Introduction

2.2 This is a joint Systems Acquisition and Development Policy. Where "The Organisation" is referenced, this refers to either Public Sector Partnership Services (PSPS) or its Client Council's South Holland District Council, East Lindsey District Council or Boston Borough Council.

2.2.1 PSPS and its clients benefit from reliability, stability and purposeful development and innovation of its systems, infrastructure, and information management.

2.2.2. Collaboration between PSPS and its Client Council employees supporting these functions and end-users is vital to designing and implementing enterprise services. As, our infrastructure has become more complex the interdependencies between systems; between people; and between people and systems continues to grow. It is essential that additions and developments of the systems and services is carefully managed.

2.2.3 PSPS ICT is the primary source for all information technology systems including communication systems, information storage and processing systems, software systems and contractual relationships with vendors of such systems and services. In addition, PSPS has oversight and coordinating responsibility for all these systems and services.

2.2.4 The purpose of this Systems Acquisition and Development Policy is to manage technological innovations and initiatives within the Organisation to ensure such changes are managed in a rational and predictable manner so that they confirm to existing guidelines to maximise functionality whilst minimising effort.

## Responsibilities

| Role | Responsibility |
|---|---|
| The Organisation's Chief Executive | Supporting Company/Authority compliance with the policy |
| Senior Management Team | Ensuring the policy adheres to statutory legislation & guidance and that it is embedded in the workforce and ensuring managers and Team Leaders show compliance with the policy and it is understood. |
| Managers & Team Leaders | Understanding and complying with the policy, ensuring it is available to team members, and advising on it. |

| | |
|---|---|
| All Staff | Understanding and complying with the policy |

# 3. Policy Statement

## Information Systems: Acquisition

## Assurance

3.1 All new Information Systems must be formally requested, and implementation approved by SLT or the ICT Strategy Board. The ICT Strategy Board compromises of senior leaders from the organisations.

3.1.1 Submission of requests is made following The Organisation's submission process. The request should include a business case, costing model, risk assessment and impact assessments and details of how the request aligns with the Organisation's strategic direction.

3.1.2 All ICT systems must be formally approved to ensure that they are aligned with the Organisation's strategic direction.

3.1.3 All Cloud Hosted ICT systems must comply with the NCSC Cloud Security Principles relating to the security of 3rd party hosted applications.

3.1.4 Full due diligence checks will be undertaken to ensure any new systems is secure, fit for purpose and complies with Organisation's data management requirements. Similar due diligence checks apply to on premise or hosted acquisitions. Such diligence might include:

- Company Background Check
- Crime prevention through environmental design policies
- Understanding of Technical considerations, including service levels.
- Service Organisation Control (SOC) Audit
- Review of Support systems.
- Statement of continued interoperability with support Microsoft OS and that of dependent subsystems.
- Onsite discovery.
- Disaster Recover/Business Continuity plans.
- Certification / Compliancy – NIST SP800, Cyber Essentials + or ISO27001
- Information relating to annual external Penetration test.
- References.

3.1.5 All ICT systems should be formally approved, before a system can process personal information, by the Organisation's Data Protection Officer (DPO), and a Data Privacy Impact Assessment (DPIA) completed. This is to ensure compliance with regulatory requirements as set out in the Data Protection Standard. It is the responsibility of the Head of Service to ensure a DPIA is completed.

3.1.6 All suppliers engaged with the processing of personal data must complete an Information Sharing Agreement, if required by the DPO. This includes software that may be downloaded and/or purchased from the Internet.

3.1.7 Under no circumstances should personal or unsolicited software (this includes screen savers, games, and wallpapers etc.) be loaded onto a Council machine as such actions significantly increase the potential of malware being introduced onto the Organisations operating environments.

## Software Registration/Licensing

3.2 The Organisation uses software in all aspects of its business to support the work carried out by its employees. In order to comply with software licencing regulations, it is essential that all software that is required to be licensed is licensed and that the licenses remain current and valid for the duration of the use of the software.

3.2.1 All software and licenses must be procured, checked, and tested by the ICT Department. In order to maintain our security standard and PSN compliance, all software must be supported and kept up to date, at least current version -1, in respect to the operation version used.

3.2.2 Software must be registered in the name of the Organisation and the department in which it will be used. Details of the license should be stored securely, ideally within the ICT Halo system, and be made available at the behest of ICT in the event of a licensing audit.

3.2.3 Only licensed software is to be installed computer equipment. Failure to hold correct software licensing can result in significant financial penalties, as such the organisation will not condone the use of unlicensed or incorrectly licensed software.

3.2.4 The ICT Service Desk maintains a register of all Organisational software and will keep a library of software licenses. The register must contain:

a) The title and publisher of the software.
b) The date and source of the software acquisition.
c) The location of each installation as well as the serial number of the hardware on which each copy of the software is installed.
d) The software product's serial number.
e) Details and duration of support arrangements for software upgrades.

3.2.5 Software on Local Area Networks or multiple machines shall only be used in accordance with the licence agreement.

3.2.6 The Organisation holds licences for the use of a variety of software products on all Organisation Information Systems and computer equipment. This software is owned by the software company and the copying of such software is an offence under the Copyright, Designs and Patents Act 1988, unless authorised by the software manufacturer.

## Software Installation

3.3 Software must only be installed by members of the ICT department once the registration requirements have been met. Once installed, the original media will be kept in a safe storage area maintained by the ICT department.

3.3.1 Shareware, Freeware and Public Domain Software are bound by the same policies and procedures as all other software. No user may install any free or evaluation software onto the Organisation's systems without prior approval from the ICT department.

## Security of Third-Party Access

3.4 Arrangements involving third party access to the Organisation's information, or information processing facilities, must be supported by a formal agreement that describes appropriate security controls and gives the Organisation the right to monitor and revoke access. Only individuals authorised by the Organisation are permitted access to the information processing facilities and only for agreed purposes. Only PSPS standard remote access methods will be permitted, and the requirement must be supported by a risk assessment detailing any associated countermeasures. All Contractors using the system must be vetted to an appropriate level that meets the Organisation's policy.

## Outsourcing

3.5 Any outsourcing arrangement must be fully supported by a formal contract and must meet legal requirements. The contract must define the appropriate organisational and technical security controls that are in place to protect the integrity and confidentiality of the information assets, including the issue and return of information, information access control, and the right to audit.

3.5.1 It should also include a requirement to support the contracting Organisation with requirements to comply with any data requests, such as data subject rights or breach management.

## Location

3.6 Location of data should be held within a secure datacentre preferably within the United Kingdom or if necessary, within the European Union.

## Asset Clarification and Control

3.7 Any new system must be purchased through the ICT Department or relevant procurement team (with ICT involvement) and recorded in the asset register. The system

must have a nominated owner who is responsible for ensuring that the agreed security controls are properly maintained and that operating procedures are being followed.

## People Security

3.8 The Data Privacy Impact Assessment must define risks and mitigation relating to all Employees and Contractors using the system. Such mitigation may include DBS checks, pre-employment credit checks, information sharing agreements or non-disclosure agreements.

3.8.1 The requirement for any additional end-user training in the use of a new system must be identified and planned for, at the initiation of the project.

3.8.2 Developers, administrators, and users of the system must immediately report any security incidents, malfunctions, or suspected security weaknesses, to the PSPS ICT department.

## Operating System Interoperability

3.9 All ICT systems should have a statement of continued development to maintain interoperability with supported Microsoft operating systems. No ICT system should require to be maintained on a non-supported OS or have components which are no longer updated for vulnerabilities by the vendor.

3.9.1 All ICT system vendors must provide a roadmap or similar document to show their commitment of continued development of the product for the lifetime required. This may include additional charges which must be included in the Total Cost of Ownership (TCO) of the product.

## Physical and Environmental Security

3.10 All information systems must be secured in an appropriate area, using physical barriers that are commensurate with the identified risks. PSPS ICT Datacenters conform to the following standards, and it is expected that any supplier would have a minimum of these controls:

- External walls of buildings and enclosures are of a solid construction with external doors and windows protected against unauthorised access using suitable control mechanisms, such as proximity card access, security locks and alarms.
- There are staffed reception areas or other physical access controls to the site or building.
- Access is restricted to authorised personnel only, with access rights regularly reviewed.
- Visitors are supervised or appropriately vetted, and their date and time of entry and departure recorded.

3.10.1 Environments housing particularly critical or sensitive systems must be individually risk assessed.

3.10.2 Equipment should be located where there is minimal risk from potential environmental and security threats, including theft, fire, water, dust, vibration, electrical interference, and chemical effects. There should be suitable protection for equipment used or housed in external environments, e.g., protective covers, locks, etc. It must be possible to position end devices and any output media so as not to risk the overlooking of sensitive information by unauthorised personnel. For operationally critical systems, suitable power protection must also be provided; to include at least one of the following: -

- Multiple power units with redundancy
- Uninterruptible Power Supply (UPS)
- Back-up generator

3.10.3 UPS and back-up generators should be operationally tested at least annually.

3.10.4 Power and telecommunications lines must be suitably protected from unauthorised access or damage.

3.10.5 All end user devices are configured to require the submission of a user ID and password to access them. In the event of having to leave a device unattended, even for a few seconds, the end user must either logout of the device or lock the device so that the screensaver with password protection is showing.

## Communications and Operations Management

3.11 System/Security Operating Procedures must be fully documented. These should include the processing and handling of information, system start-up and shutdown procedures, account management, support & maintenance, data retention, data backup, and business continuity plans (e.g., fallback procedures).

3.11.1 Any changes to the systems must be performed in accordance with the Change Management Policy. Changes must be logged, via Halo. The ICT Change Advisory Board (CAB) will access any security risks as part of a formal approval process. Implementation of changes must be planned for a time that causes the minimum disruption to the Organisation. There should be a proper separation of development/test and production environments and live data should not be used for test or development scenarios. Different login-procedures must exist between environments to minimise the risk of accidental changes to operational systems.

3.11.2 Appropriate anti-virus measures are in place. Anti-Virus signatures must be regularly and securely updated to protect end user devices, systems, connections, and data.

3.11.3 A procedure for the backing-up of essential system information and software must be defined and adequate logs maintained. The backup media must receive the same level of protection as the main system and should be kept at a sufficiently safe distance to protect against the risks caused by its unavailability. These procedures must include a regime of regular testing to ensure that data can be reliably restored.

3.11.4 All systems must provide appropriate mechanisms to facilitate the timely removal of data in accordance with relevant Organisational policy and current legislation.

3.11.5 All systems must provide appropriate mechanisms to retrieve personally identifiable data for subject access requests.

3.11.6 The network design must provide an appropriate level of resilience for the system(s) and minimise single points of failure. The network must be protected from increased security risks introduced by any connections to other systems, particularly connections to public networks.

3.11.7 Network documentation must be updated to show any supporting changes to the network's layout or connections. New network management responsibilities must be properly assigned, and procedures documented. All network device settings must be changed from their default values to PSPS standard configurations, and any unnecessary facilities and services disabled or locked down.

3.11.8 There must be clearly documented procedures that cover the safe handling and storage of all removable media, including tapes, disks, manuals, and printouts. Organisational policy on the handling of material must be followed at all times. Provision must be made for ensuring that any data storage media used for processing information is securely erased in accordance with the Organisation's policy before reuse, exchange, or disposal.

3.11.9 Any exchange of information or software with another Organisation must be supported by a formal, documented agreement that complies with relevant policy and legislation (Contact the Data Protection Officer for assistance).

3.11.10 External-facing systems, especially Internet and publicly available systems, must have adequate controls to protect against their particular vulnerabilities. These often involve more technical controls, such as cryptographic techniques, and the risks and countermeasures must be clearly defined within the system's Risk Assessment. Other effects on the Organisation from switching to electronic methods of communication, such as the volume of exchange, reliability, or legal issues, also need to be risk assessed.

3.11.11 Internal systems must ensure that access to data and facilities is only made available to those who need it, particularly in relation to personal data or classified business information.

## Access Control

3.12 Access to information and processes for each user or group must be clearly defined and documented. Access control rules must be based on the principle that 'everything not explicitly permitted is prohibited'.

3.12.1 A unique ID must be provided for each user of the system. Generic log-in rights are not acceptable, even at System Administrator level. Access rights must be agreed by the system owner (Information Asset Owner).

3.12.2 Procedures must also be defined for removing access rights immediately they are no longer required and for regularly checking and removing any redundant accounts (every 6 months is recommended).

3.12.3 The use of any system privileges (the ability to override system controls, e.g., for administration) must be restricted to the minimum necessary to perform a defined role. Such

privileges are not usually granted to normal business users and must be reviewed regularly (every 3 months is recommended).

3.12.4 A full log of registered users and administrators and their access rights must be maintained by the system owner (Information Asset Owner) and made available for audit.

3.12.5 Passwords must always be stored and transmitted securely using approved encryption. On first use, the system must force a change of any temporary passwords that were issued to the user. Positive user identification procedures must be established for resetting forgotten passwords. The system's risk assessment may also identify the need for strong authentication techniques, including multi-factor solutions.

3.12.6 Where possible, Single Sign-On technology should be available and used to integrate into the Organisation's Authentication protocols.

3.12.7 It must be possible for users to easily terminate or secure active sessions (e.g., by password protected screen saver) before leaving a device unattended.

3.12.8 Any connections to internal or external network services that are implemented for the system must be appropriately controlled and provided for authorised use only. The path from the user device to the system must be controlled to ensure that no other areas of the system or network are made accessible, outside that which has been authorised.

3.12.9 Any requirement for external access to the system (e.g., for maintenance or support purposes) must be fully risk assessed. Solutions must comply with agreed standards and procedures governing remote connections including legislation and current guidance regarding transfer of data outside the UK and EU.

3.12.10 Where a system requires a level of protection that is generally outside that of the main network, such as managing more sensitive information or needing higher risk external connections, it may be necessary to segregate the system into a separate physical or logical network domain (an isolation environment), rather than adjust controls for the existing network. Controls for network connections must be fully specified, particularly when routing information to and from other Organisation's, e.g., host authentication and network address translation.

3.12.11 Any other network services required (or planned) for the system must be fully risk assessed and documented.

3.12.12 Device log-on procedures must be clearly documented. The system log-on procedure must:

- not identify details about the system nor provide any other help to unauthorised users during the log-on process.
- display a warning that it must only be accessed by authorised users.
- not provide details of which part of a failed log-on procedure was incorrect.

3.12.12 The system must limit unsuccessful log-on attempts to 3, after which the account must lock and require a manual reset.

## Monitoring System Access and Use

3.13 Audit logs must be maintained that record user access events. The logs must be protected and routinely inspected by appropriate personnel. Suitable tools should be specified to assist in the analysis and alerting of key log events. Computer clocks must be synchronized for accurate recording of time sensitive records, such as log entries.

## Mobile Computing

3.14 Mobile working systems are particularly vulnerable and specific security controls must be identified following risk assessment. The use of mobile working facilities must comply with the Organisation's standards, policy, and procedures wherever possible.

# Information Systems: Development and Maintenance

## Security Requirements of Systems

3.15 The requirements and designs for new or changed systems must be formally documented and state the security controls that are being implemented. There must be a sufficient level of detail provided in the Request for Change to allow a thorough assessment of any associated application's security architecture and configuration. A Data Privacy Impact Assessment should be considered when developing systems containing personal data.

3.15.1 Changes to any operational software must be controlled through the Change Advisory Board (CAB) to ensure that no unacceptable risks are introduced to any system. The Company's Information Technology Service Management tool (ITSM), Halo, must be updated with details of any system changes. Documented test plans must be created and approved before any test data is copied and used. All testing must be carried out under conditions that match that of the intended production environment and all test results must be formerly recorded. Appropriate test data must be identified and produced for all system testing - production data must not be used for testing. Vendor-supplied software must have been properly evaluated, using a formal test plan, prior to any agreement to purchase. The test results must be formally documented.

3.15.2 System changes must be supported by a full audit trail and follow the Organisation's procedures for ensuring that security risks are reassessed as part of a formal approval process. This must include version control for all software updates. The implementation of system changes must be managed through the ICT Change Advisory Board. Changes to vendor-supplied software must be kept to the minimum necessary, be authorised by the vendor and preferably implemented by the vendor as a standard update. Any associated future support issues must be resolved before implementation. There must be proper provision for the timely review and updating of any necessary operating system changes (e.g., patching). For outsourced developments, advance agreement must be reached over the issues surrounding licensing, code ownership, the Organisation's right to audit quality and accuracy, and any necessary contractual arrangements.

## Business Continuity Management

3.16 There must be a formal evaluation of how and where the system needs to support the organisation's overall business continuity plan and appropriate technical and procedural controls will need to be specified.

3.16.1 Appropriate controls and procedures must be in place to allow the system to reliably recover in the event of a system failure.

3.16.2 Disaster recovery plans must be documented and specify contingency plans or manual processing procedures that must be followed in the event of an extended loss of the system. These plans must be regularly tested.

## Compliance with Legal Requirements

3.17 The design, operation, use and management of an information system must comply with statutory, regulatory, and contractual security requirements. Where the system will be used to process personal data, appropriate security controls must be specified in order to comply with current legal requirements.

3.17.1 In addition, any introduction of a system must have been revised by the Organisation's DPO and a complete Data Privacy Impact Assessment conducted and documented.

3.17.2 For proprietary systems or software, a license agreement that clearly states the terms and conditions of use must be obtained. The agreement must be thoroughly reviewed and accepted before implementation and copies of the agreement and proof of ownership must be maintained.

## System Audit

3.18 The system must support regular system security and data audits to ensure compliance with policy and legislation. Any logging facility must be protected from unauthorised deactivation or unauthorised changes. The log media must also be protected from becoming exhausted or over-written before it meets the agreed disposal date.

# 4. Review

4.1 As a standard principle, this policy should be reviewed at least once every three years to ensure that it remains fit for purpose. It may need reviewing more regularly in response to specific legislation changes or changes to best practice guidance.

# 5. Policy Compliance

5.1 If any user is found to have breached this policy, they will be subject to the Organisation's disciplinary procedure. If a criminal offence is considered to have been committed further action may be taken to assist in the prosecution of the offender(s).

5.1.1. If you do not understand the implications of this policy or how it may apply to you, seek advice from the ICT Department.

# 6. Related Policies

Data Protection Standard

Change Management Procedure

Employers Code of Conduct

Employers Disciplinary Policy