PSPS
Public Sector Partnership Services Ltd

Delivering services for South Holland District Council, Boston Borough Council, East Lindsey District Council

Appendix D

Information Security Policy
Third Party Access

May 2021

Document Control

Version Control

Issue Number	Issue Author	Issue Date	Reason for Issue
1.0	J Wright	Oct 18	New Policy for review
1.1	J Wright	Jan 19	Revised to incorporate SHDC DPO requirements
1.2	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

Approval Control

Issue Number	Approval Authority	Name	Approval Date	Due for Review
3.1	ELDC/BBC	James Gilbert	May-21	May-24
	PSPS	Lewis Ducket	May-21	May-24
3.2	SHDC	James Gilbert		May-24

Contents

1. Policy Aim

The purpose of this policy is to clarify the procedures and responsibilities with regard to initiating a new connection between the Organisation and a third party Organisation or service provider in order to maintain confidentiality, integrity and availability.

Responsible	Head of ICT & Digital
Accountable	Chief Executive (PSPS), Executive Director (SHDC), Assistant Director (ELDC/BBC)
Consulted	Data Protection Officers, ICT Security Lead
Informed	All ICT Users including third parties and supervising users

2. Definition

Third parties are defined as any individual or Organisation not employed directly by the Organisation and includes partners such as the NHS, Police and other local authorities. It also includes suppliers who require access to the Organisation's network to provide remote support.

This policy applies to all existing and new permanent or temporary connections and applies to any connection agreement with a third party. Any sanctions and obligations specified within the contract may be imposed as part of the third party connection agreement.

3. Introduction

This is a joint Employee Access Policy. Where "The Organisation" is referenced, this refers to either Public Sector Partnership Services or its Client Council's South Holland District Council, East Lindsey District Council or Boston Borough Council.

The Organisation permits connections to third party Organisation's to promote partnership working, information sharing, service provision and support arrangements with third party Organisation's or service providers. This policy is specific to the authority's requirements when establishing new links between the Organisation and third parties and makes reference to additional security policies and procedures.

This Third Party Policy forms part of the Information Security Framework.

4. Roles and Responsibilities

The following roles are those formally defined within the Policy:

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.

5. Policy Statement

The overall security of the Organisation's infrastructure, systems and data takes precedence over any individual requirements for a third party connection.

A specific business purpose must exist and be defined for a third party connection to be considered. For each third party connection agreement, named lead persons responsible for the system and information concerned must be appointed by both the Organisation and third party.

A risk assessment should be conducted, prior to implementation of any connection, to identify specific requirements. It will be the responsibility of the named Organisation lead person to carry out the assessment. The risk assessment will consider:

- A description of the participants in the assessment.
- The type of access required and the data that needs to be available to the third party.
- The value and sensitivity of information and information systems that may be exposed to unauthorised access.

- The threat and vulnerability (the risk) to information and information systems and the impact if the threat were to take place.
- The controls required to protect information and information systems. An overview of the users.
- How the third party Organisation manages and controls information security
- Details of how the third party will secure their ICT equipment and networks.
- The method of access required – physical and logical connectivity between information systems.
- Dates of when the access is required from and a cessation date if a temporary arrangement. If a permanent arrangement is required, then an annual review must be incorporated in the agreement.
- Security incident management.
- Legal requirements affecting stakeholders.
- A statement assessing and listing all risks.
- The requirement for a formal Data Privacy Impact Assessment.
- An overall conclusion.

Any third party Organisation with which the Organisation enters into a connection agreement must be able to demonstrate compliance with the information security policies and enter into binding agreements that specify the performance to be delivered and the remedies available in the event of non-compliance.

The Organisation point of contact will:

- Have administrative responsibilities.
- Draft a non-disclosure agreement/information sharing agreement.
- Be responsible for remote access provision.
- Act as a point of liaison both with the third party and the ICT Department.
- Be responsible for ensuring background checks (such as DBS and Baseline Personnel Security Standard) are made on individuals utilising services/information provided by the connection.
- Ensure all relevant bodies are informed when the connection is no longer required.

The Third Party point of contact will:

- Be responsible for managing all aspects of the connection on behalf of the third party.
- Be the primary point of contact and be able to provide accurate information on all aspects of the third party.

- Ensure that all third party users have received appropriate training and have under-gone appropriate background checks.

Third party access to the ICT network potentially exposes the Organisation to risk and therefore there must be an agreement in place that assures the Organisation that any third party connection meets the security standards. The third Party must consider and address:

- A description of services and service level agreement.
- Reference to relevant security policies and legislation.
- Requirements for asset protection and access control.
- Responsibilities and liabilities.
- Monitoring rights and reporting processes.
- The minimum ICT security rights to support the system.
- Conditions for termination and renegotiation of agreements.

If a log of third party activity on the Organisation's network is required as part of the agreement, then the third party will need to retain this log for the period specified in the agreement. Remote access software must be disabled when not in use.

All third party access must be facilitated through a method of connection approved by the Organisation which provides protection to the satisfaction of the Organisation. All third party access must be logged via the ICT Service Desk and duly authorised before being permitted onto the network. Once authorisation has been obtained a time restrictive username and password should be provided.

Changes to methods of connection must be clearly defined and agreed by the Organisation and the third party.

Third parties and the Organisation must inform each other about any security incidents which may impact on the confidentiality, integrity or availability of the third party service or data provided by the service. Incidents originating within the Organisation must be handled in accordance with the ICT Security Incident Management Policy.

The range of security incidents which will require security awareness procedures include:

- Computers left unlocked when unattended;
- Password disclosures;
- Virus warnings/alerts;
- Media loss;
- Data loss/disclosure;

- Misuse/loss/corruption/alteration of personal information;
- Physical security;
- Missing correspondence;
- Found correspondence/media;
- Loss or theft of IT/information; and
- Misuse of IT equipment/facilities.

Third parties with whom the Organisation has a third party connection contract are permitted access only to systems and information related to that contract. All other access is prohibited. Any third party with access to sensitive authority information must be cleared to the same security and human resources checks as Organisation's staff.

6. Responsibilities

It is the responsibility of the Organisation and each third party to ensure that all sections of this policy are adhered to.

Should changes in the requirements of either the Organisation or the third party regarding the connection become apparent, such as:

- Life span of the service;
- Changes in the information required;
- Changes in the type of connection;
- Changes in any aspect of security;
- Changes of key contacts; and
- Emergency handling procedures.

Each party should notify the other as soon as possible and the respective connection agreement should be revised.

7. Review

As a standard principle, this policy should be reviewed at least once every two 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.

8. Policy Compliance

The Organisation and third parties will abide by all UK legislation relating to information storage and processing including:

- The Data Protection Act (2018)
- The General Data Protection Regulation (2016/679)
- The Freedom of Information Act (2000)
- The Computer Misuse Act (1990)
- The Human Rights Act (1998)
- The Copyright, Designs and Patents Act (1988)
- The Regulation of Investigatory Powers Act (2000)
- The Electronic Communications Act (2000)
- Privacy and Electronic Communications Regulations (2003)

The Organisation and third parties will also comply with any contractual requirements, standards and principles required to maintain the business functions of the authority including:

- Protection of intellectual property rights;
- Protection of the authority's records;
- Compliance checking and audit procedures;
- Prevention of facilities misuse;
- Relevant codes of connection to Third Party networks and services.

Breaches of third party connection agreements and/or security incidents can be defined as events which could have, or have resulted in, loss or damage to Organisation's assets, or an event which is in breach of the security procedures and policies.

The Organisation will take appropriate measures to remedy any breach of a third party connection agreement. If a breach/security incident relates to a third party the Organisation reserves the right to immediately terminate the third party connection and, subject to the nature of the breach/security incident, seek compensation or take legal action. If it can be determined that the breach/security incident has been caused by an employee of the third party, the Organisation would retain the right to request the employer to remove their employee from the premises.

If the breach/security incident is determined to have been caused by an individual employed by the Organisation, the matter may be dealt with under the 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).

9. Related Policies

Information Security Framework Overview

Acceptable Use Policy

Employee Access Policy

Password Policy

Remote Working Policy

ICT Incident Management Procedure

Systems Acquisition, Development and Deployment Policy

Employers Code of Conduct

Employers Disciplinary Policy