Committee report

Information and Cyber Security Policies

Committee Personnel

Date of meeting 5 November 2021 **Date of report** 12 October 2021

Report by Director of Finance

1. Object of report

The object of this report is to recommend approval of the Information and Cyber Security policies within Appendix 1 and Appendix 2.

2. Background

SPT uses Information Technology (IT) to support all aspects of service delivery. Information and cyber security policies play a central role in ensuring the success of SPT's cybersecurity strategies and efforts. A security policy identifies the rules and procedures that all individuals accessing and using an organisation's IT assets and resources must follow. The goal of these security policies is to support the mitigation of cyber security risks as well as defining how to recover when an incident occurs. Furthermore, the policies provide guidelines to employees on what to do and what not to do.

3. Current position

Currently, SPT has policies in place governing Information Security. These policies require to be updated so that they conform to requirements of the Scottish Government Cyber Resilience Framework (SCRF). SPT has compliance obligations pertaining to Payment Card Industry (PCI) accreditation, in which SPT are required to keep current and relevant in order to gain accreditation for the processing of payment card details.

4. Proposal

SPT's proposed new security polices will define roles and responsibilities, outlining who is responsible for which task, who is authorised to do such a job, what one employee can do and cannot do. Any onboarding employee can be quickly acquainted with SPT's rules and regulations. They define not only the roles and responsibilities of employees but also those of other people who use SPT's resources (like guests, contractors, suppliers, and partners).

The policies will increase employee cyber security awareness, as they will act as educational documents, covering a range of topics critical to the security of SPT's technology.

Critically these security policies will shape SPT's cyber security efforts, ensuring SPT is compliant with the SCRF and PCI requirements.

The proposed Information and Cyber Security policy statement, and supporting policy, are the first documents in a suite of framework documents designed to address the organisations information security governance requirements. These policies will be supported by appropriate standards, guidance and procedural documentation, where required.

5. Recommendation

The committee is asked to approve the associated 'Information and Cyber Security Policy Statement' and, 'Information and Cyber Security Policy'.

6. Consequences

Policy consequences	*Replaces Information Security Policy Statement & IT User Guide.*
Legal consequences	*None directly*
Financial consequences	*PCI generates fines without accreditation*
Personnel consequences	*Policies will directly affect personnel*
Equalities consequences	*None directly*
Risk consequences	*Revised policies will support the mitigation cyber risks*

Name	Neil Wylie	**Name**	Valerie Davidson
Title	**Director of Finance**	**Title**	**Acting Chief Executive**

For further information, please contact *Callum Campbell* on *07385 464022 or callum.campbell@spt.co.uk.*

Strathclyde Partnership for Transport

Information & Cyber Security Policy Statement

Page	Version	Date	Purpose/Changes	Initials
All	0.01	16/07/2021	Evolution of Information Security Policy Statement	CC
All	0.02	17/08/2021	Accepted changes	CC
All	0.03	04/10/2021	Feedback changes	CC
All	0.04	05/10/2021	Version sent for senior management review	CT/CC
All	0.05	20/10/2021	Formatting	CC
All	1.0		New version 1	CT/CC

Contents

1. Statement

Strathclyde Partnership for Transport (SPT) Management has established an Information & Cyber Security Policy Statement, which supports the strategic aims of the business and is committed to maintaining and improving information security within SPT as well as minimising its exposure to threats and risks. It is therefore SPT policy to:

a. Ensure the confidentiality of all information;
b. Maintain the integrity of all information;
c. Ensure the availability of information, as required;
d. Provide information (management) security training for staff relative to roles;
e. Meet the expectations and requirements of all interested parties, in relation to Information Security;
f. Meet all regulatory and legislative requirements, and;
g. Communicate this policy statement to the public on request.

2. Scope of Statement

This statement is aimed at all entities pertaining to SPT's information & cyber security.

3. Functional Responsibilities

3.1 Executive Management is responsible for:

3.1.1 Committing to manage risks arising from cyber threats;

3.1.2 Ensuring appropriate policies and processes are in place to direct SPT's approach to information security;

3.1.3 Defining clear lines of responsibility and accountability to named individuals for the security of sensitive information and key operation of services;

3.1.4 Ensuring senior management have received appropriate training and guidance on cyber security and risk management;

3.1.5 Promoting a culture of awareness and education about cyber security across SPT;

3.1.6 Ensuring risks to sensitive information and key operational services are identified and managed;

3.1.7 Ensuring there are clear and well-understood channels for communicating and escalating risks;

3.1.8 Adhering to specific legal and regulatory requirements related to information security;

3.1.9 Communicating legal and regulatory requirements to the designated security representative; and

3.1.10 Communicating requirements of this policy and the associated SPT guidance, including the consequences of non-compliance, to the workforce and third parties, and addressing adherence in third party agreements.

3.2 Digital Management is responsible for:

3.2.1 Supporting security by providing clear direction and consideration of security controls in the data processing infrastructure and computing networks and products which support the information owners;

3.2.2 Identifying and coordinating relevant processes, policies and controls relative to security requirements defined by SPT and this policy;

3.2.3 Implementing the proper controls for information owned based on the classification designations;

3.2.4 Providing training to appropriate technical staff on secure operations;

3.2.5 Fostering the participation of information security and technical staff in protecting information assets, and in identifying, selecting and implementing appropriate and cost-effective security controls and procedures; and

3.2.6 Overseeing the implementation of technology-based business continuity and disaster recovery plans.

3.3 Cyber Security and Continuity Lead is responsible for:

3.3.1 Maintaining familiarity with business security functions and requirements;

3.3.2 Maintaining an adequate level of current knowledge and proficiency in information security through annual Continuing Professional Development directly related to information security;

3.3.3 Assessing compliance with information security policies and legal and regulatory information security requirements;

3.3.4 Evaluating and understanding information security risks and how to appropriately manage those risks;

3.3.5 Representing and assuring security architecture considerations are addressed;

3.3.6 Advising on security issues related to procurement of products and services;

3.3.7 Escalating security concerns that are not being adequately addressed according to the applicable reporting and escalation procedures;

3.3.8 Disseminating threat information to appropriate parties;

3.3.9 Participating in the response to potential security incidents;

3.3.10 Participating in the development of enterprise policies and standards that considers the SPT's needs;

3.3.11 Promoting information security awareness; and

3.3.12 Ensuring sufficiency of management information for the performance management of cyber security.

3.4 Separation of Duties

3.4.1 To reduce the risk of accidental or deliberate system misuse, separation of duties and areas of responsibility must be implemented where appropriate and possible;

3.4.2 Whenever separation of duties is not technically feasible, other compensatory controls must be implemented, such as monitoring of activities, audit trails and management supervision;

3.4.3 The audit and approval of security controls must always remain independent and segregated from the implementation of security controls.

4. Review

This policy is not intended as a stand-alone document and is supported by detailed policy, guidance and process operating procedures, to form a set of working documents, which define SPT's security activities. Further information for all staff including responsibilities is available within SPT's *Information Technology & Cyber Security Policy*. Cyber security policies will be reviewed annually.

5. Approval

Signature: Print:

Date: Designation:

Strathclyde Partnership for Transport

Information & Cyber Security Policy

Page	Version	Date	Purpose/Changes	Initials
All	0.01	16/07/2021	Evolution of IT and Information Security Policy	CC
All	0.02	18/08/2021	Accepted changes	CC
All	0.03	04/10/2021	Feedback changes	CC
All	0.04	05/10/2021	Version sent for senior management review	CT/CC
All	0.05	19/10/2021	Formatting	CC
All	1.0		New version 1	CT/CC

Contents

1. Statement of Policy

This policy is the central information security policy for all digital and information assets associated with SPT. It defines the mandatory minimum information and cyber security requirements for SPT.

2. Scope of Policy

This policy applies to all SPT employees, partners and contractors. This document applies to all systems, automated and manual or hosted by third parties on behalf of SPT.

3. Associated Legislation

This policy and the associated documents are designed to be consistent with the following legislative acts;

a. *Data Protection Act 2018*
b. *Computer Misuse Act 1990*
c. *Telecommunications Act 1984*
d. *Regulation of Investigatory Powers Act 2000*

4. Associated Documents

The following documents support this policy;

a. *Acceptable Use Procedures (Digital Assets)*
b. *Digital System Security Standards*
c. *Information & Cyber Security Risk and Recovery Standards*
d. *PCI-DSS Subway Standards*

5. Policy Responsibility Statement

5.1 SPT Staff, Partners and Contractors Responsibilities;

5.1.1 Understanding the baseline information security controls necessary to protect the information entrusted;

5.1.2 Protecting information and resources from unauthorised use or disclosure;

5.1.3 Protecting OFFICIAL, OFFICAL/SENSITIVE or SECRET information from unauthorised use or disclosure, and;

5.1.4 Reporting suspected information security incidents or weaknesses to the appropriate manager and designated security representative.

5.2 Clear Desk:

5.2.1 Employees are required to ensure that all OFFICIAL, OFFICAL/SENSITIVE or SECRET information in hardcopy or electronic form is secure in their work area at the end of the day and when they are expected to be absent for an extended period;

5.2.2 Computers must be locked when workspace is unoccupied, and shut down at the end of working day;

5.2.3 Any OFFICIAL, OFFICAL/SENSITIVE or SECRET information must be removed from the desk and locked in a drawer when the desk is unoccupied and at the end of the work day;

5.2.4 File cabinets containing OFFICIAL, OFFICAL/SENSITIVE or SECRET information must be kept closed and locked when not in use or when not attended;

5.2.5 Keys used for access to OFFICIAL, OFFICAL/SENSITIVE or SECRET information must not be left at an unattended desk;

5.2.6 Passwords may not be left on sticky notes posted on or under a computer, nor may they be left written down in an accessible location;

5.2.7 Printouts containing OFFICIAL, OFFICAL/SENSITIVE or SECRET information should be immediately removed from the printer;

5.2.8 Upon disposal OFFICIAL, OFFICAL/SENSITIVE or SECRET documents should be shredded in the official shredder bins or placed in the lock confidential disposal bins;

5.2.9 Treat mass storage devices such as CDROM, DVD or external USB drives as OFFICAL/SENSITIVE and secure them in a locked drawer.

5.3 Bring Your Own Device (BYOD)

5.3.1 Devices not supplied or approved by SPT are not permitted connection to SPT's networks or services.

5.4 Passwords

5.4.1 All user-level and system-level passwords must conform to Password Construction Guidance found in the *Acceptable use Procedures*;

5.4.2 Users must use a separate, unique password for each of their work-related accounts. Users may not use any work-related passwords for their own, personal accounts;

5.4.3 User accounts that have system-level privileges have a unique password from all other accounts held by that user to access system-level privileges;

5.4.4 Passwords must not be shared with anyone, including managers and co-workers, all passwords are to be treated as OFFICAL/SENSITIVE SPT information;

5.4.5 Passwords must not be inserted into email messages or other forms of electronic communication, written on paper, nor revealed over the phone to anyone, unless approved by the Digital manager;

5.4.6 Do not use the "remember password" feature of applications (for example, web browsers) and;

5.4.7 Any user suspecting that their password may have been compromised must report the incident immediately and change all passwords.

5.5 Acceptable Use Procedures (AUP)

5.5.1 AUP's apply to all SPT employees and members, including temporary staff, suppliers and contractors, with access to Digital assets, SPT e-mail, intranet and internet resources. Further information pertaining to AUP's, refer to *SPT's Acceptable Use Procedures.*

5.6 Removable Media

5.6.1 The only devices and media permitted to connect to SPT's equipment or networks and systems, is equipment purchased by SPT and approved by the Digital manager with an appropriate business case;

5.6.2 SPT has obligations under Freedom of Information and Data Protection (including security and retention). Therefore, only SPT issued removable media devices must be used to store information used to conduct official SPT business;

5.6.3 Unless approval is granted by the Digital manager with an appropriate business case, SPT issued removable media devices must not be connected to any device that is external to SPT's network, and;

5.6.4 Removable media devices must only be used for work purposes.

5.7 Physical Access Control

5.7.1 Only authorised personnel with an approved business case are permitted restricted area access containing information systems. Authorised personnel must follow policies and procedures ensuring security of restricted systems and areas.

5.8 Remote Working

5.8.1 Authorised users shall protect their login and password, even from family members;

5.8.2 Connecting to an SPT network or system must be made using an SPT pre-configured VPN (Virtual Private Network);

5.8.3 Whilst using an SPT owned device to remotely connect to SPT's corporate network, authorised users shall ensure the device is not connected to any other network at the same time, with the exception of personal networks that are under their complete control or under the complete control of an authorised user or third party;

5.8.4 Use of external resources to conduct SPT business must be approved in advance by the appropriate business unit manager;

5.8.5 Personal equipment used to connect to SPT's networks externally is not permitted, and;

5.8.6 Utilisation of third-party software on a personal device to connect to an SPT service is not permitted.

5.9 System Security

5.9.1 Those in specialised roles are required to adhere to polices, guidance and procedures pertaining to digital system security, refer to the *Digital System Security Standards.*

5.10 Risk and Recovery

5.10.1 Those in specialised roles are required to adhere to polices, guidance and procedures pertaining to cyber security risk and disaster recovery/business continuity, refer to Cyber *Security Risk and Recovery Standards.*

5.11 Payment Card Industry Data Security Guidance (PCI-DSS)

5.11.1 Where specialised roles are required to adhere to polices, guidance and procedures pertaining to Payment Card Industry Data Security Standards (PCI-DSS), refer to the *PCI-DSS Subway Standards.*

6. Compliance

Compliance is expected with all SPT policies, guidance and procedures. Policies, guidance and procedures may be amended at any time. Compliance with amended policies, guidance and procedures is expected. Non-compliance with this policy may result in disciplinary action.

7. Review

This policy is not intended as a stand-alone document and is supported by detailed policy, guidance and process operating procedures, to form a set of working documents, which define SPT's security activities. This policy will be reviewed annually.

8. Approval

Signature: Print:

Date: Designation: