INFORMATION SECURITY POLICY

Contents

Document Management

Version	Name	Revision Date	Change
2.0	Peter Johnston (Citation)	07/08/2024	Rewrite following upgrade to ISO 27001:2022

Responsibility and Authority

The Smarterpay Executive holds overall authority.

Responsibility	Appointment
Periodic review and maintenance	Christopher Bell
Release approval	Christopher Bell

Purpose

Information is a vital asset to Smarterpay (SMP). This Policy concerns the management and security of SMP's information assets and the use of these assets by its members and others who may process information on behalf of SMP.

The primary purposes of this Policy are to:

- Ensure the protection of all SMP information systems and mitigate the risks associated with their theft, loss, misuse, damage or abuse.
- Make certain that users are aware of and comply with all current and relevant UK and EU legislation and customer confidentiality.
- Provide a safe and secure information systems working environment for staff and any other authorised users.
- Ensure that all SMP authorised users understand and comply with this policy and any other associated policies.
- Ensure that all users understand their own responsibilities for protecting the confidentiality and integrity of the SMP and customer data that they handle.
- Protect SMP and our customers from liability or damage through the misuse of its IT equipment.
- Respond to customer feedback and update as appropriate, initiating a cycle of continuous improvement.

Scope

The documents of the Information Security Policy apply to all information assets owned by SMP, used by SMP for business purposes or which are connected to SMP's networks.

The documents of the Information System (IS) apply to all information which the company processes, irrespective of ownership or form.

This policy is applicable to and will be communicated to all SMP staff who interact with information held by SMP and the information systems used to store and process it.

Responsibility and Authority

The Smarterpay Executive holds overall authority for this Policy.

STAFF

All SMP staff will be users of SMP information. It is the responsibility of all staff to abide by this policy and its principles and procedures. No individual should be able to access information to which they do not have a legitimate access right. Notwithstanding this, no individual should knowingly contravene this policy nor allow others to do so. It is the responsibility of all staff to protect the confidentiality of our customer's data.

DIRECTORS

Directors are responsible for the information systems, both manual and electronic, that support SMP's work. This includes ensuring that data is appropriately stored, that the risks to data are appropriately understood and either mitigated or explicitly accepted, that the correct access rights have been put in place, with data only accessible to the right people, and ensuring there are appropriate backup, retention, disaster recovery and disposal mechanisms in place.

MANAGERS

Managers are responsible for a specific area of SMP work, including all the supporting information and documentation that may include working documents, contracts and staff information.

Compliance

This Policy meets the requirements of ISO 27001:2022 Control A5.1.

Structure

This Information Security Policy document set is based on the control guidelines set out in the industry standard ISO 27001:2022.

This top-level document includes sub-policies and lists further sub-policy documents, which together constitute the Information Security Policy for SMP. Each sub-policy contains high-level descriptions of requirements and principles.

Alignment with Business Strategy

Smarterpay:

- Employs high-quality staff who can develop and comply with strict information security policies and practices.
- Invests in high-quality, secure technology.
- Produces products that incorporate leading information security technologies and techniques.
- Implements information security globally.
- Highly secures our and our customer's information.

Legal & Regulatory Obligations

Smarterpay abides by and adheres to all UK and EU legislation, including the:

- Computer Misuse Act 1990
- General Data Protection Regulation (GDPR) – see Computer user Handbook
- Freedom of Information Act 2000
- Regulation of Investigatory Powers Act 2000
- Defamation Act 1996
- Obscene Publications Act 1959
- Criminal Justice Act 1988
- Digital Economy Act 2010

The requirements of this legislation are written into our policies and procedures.

Threat Environment

Smarterpay processes confidential business and personal information for many high-profile customers. Our information is a high-value target. A national threat assessment published by CESG

Cheltenham warns that many small—and medium-sized companies are constant targets for domestic and international commercial espionage. The threat to SMP's information systems is considered high.

Information Security Objectives

Information security is the practice of protecting information from unauthorised access, use, disclosure, disruption, modification, perusal, inspection, recording and destruction.

Smarterpay's objective is to protect our information and our client's information from unauthorised access, use, disclosure, disruption, modification, perusal, inspection, recording and destruction.

Principals of Information Security

The following eight information security principles provide overarching governance for the security and management of information at SMP.

- Information should be classified according to an appropriate level of confidentiality, integrity and availability and in accordance with relevant legislative, regulatory and contractual requirements and SMP policy.
- Staff with designated roles for information management are responsible for ensuring the classification of that information, handling that information in accordance with its classification level, and any policies, procedures or systems for meeting those responsibilities. All Customer information is assumed to be CONFIDENTIAL unless they advise us otherwise.
- All users covered by the scope of this policy must handle SMP and Customer information appropriately and in accordance with its classification level.
- As far as is reasonably possible, endeavours must be made to ensure data is complete, relevant, accurate, timely and consistent.
- Information should be both secure and available to those with a legitimate need for access in accordance with its classification level.
- SMP and customer Information will be protected against unauthorised access and processing in accordance with its classification level.
- SMP and customer information will be protected against loss or corruption.

Breaches of this policy must be reported.

New Information Systems and Projects

The need for information security must be considered when considering new services and undertaking new projects.

Incident Handling

Deviations from and exceptions to our policy and processes are addressed using our incident handling and nonconformance procedures:

- SP – Information Security Incident Management Procedure.
- SP – Nonconformance Procedure.

Information Classification

The following table provides a summary of the information classification levels that have been adopted by SMP and which underpin the 8 principles of information security defined in this policy:

Security Level	Definition	Examples
CONFIDENTIAL	Disclosure has a serious impact on long-term strategic objectives. It is normally accessible only to specified members of SMP staff.	Network security information such as passwords. Payroll information
RESTRICTED	Disclosure has a significant short-term impact on operations. Normally accessible only to specified members of SMP staff.	Personal data Customer NDA Source code Sensitive business reports
CONTROLLED	Disclosure causes minor embarrassment or minor operation inconvenience. Normally accessible only to members of SMP.	Internal correspondence, papers and information held under licence.
PUBLIC	Accessible to all members of the public	Annual accounts, minutes of statutory and other formal committees, and pay scales. Information is available on websites.

Smarterpay Computer Use Handbook

Policies on the following topics are addressed in the Smarterpay Handbook:

- Physical and environmental security.
- Acceptable use of mobile devices.
- Privacy and protection of personal information.
- Password Policy.

SMP will provide staff with refresher training on the content of this Handbook at least annually or when significant new content is added.

Compliance, Policy Awareness and Disciplinary Procedures

Any security breach of SMP's information systems could lead to possible loss of confidentiality, integrity and availability of personal or other confidential data stored on information systems. The loss or breach of confidentiality of personal data is an infringement of the GDPR, contravenes SMP Data Protection Policy, and may result in criminal or civil action against SMP.

The loss or breach of confidentiality of contractually assured information may result in the loss of business, financial penalties or criminal or civil action against SMP. Therefore, it is crucial that all users of SMP's information systems adhere to this Information Security Policy and its supporting policies, as well as the Information Classification Standards.

Any security breach will be handled in accordance with all relevant SMP policies, including disciplinary policies.

Supporting Policies, Codes of Practice, Procedures and Guidelines

Supporting policies have been developed to strengthen and reinforce this policy statement. These, along with associated codes of practice, procedures and guidelines, are available on SharePoint. All staff, students and any third parties authorised to access SMP's network or computing facilities are required to familiarise themselves with these supporting documents and adhere to them in the working environment.

Supporting policies:

- SP – Access Control Policy

Records

The following records are to be used in conjunction with this procedure:

- Register of SMP System Owners.
- System Owners: Role and Responsibilities
- Training Matrix.