IS02 – Information Security Standard

Version 1.3 – May 2025

POLICY DETAILS	
Author(s)	Christine Marriott
Director Responsible	Assistant Director - DTS
Documents Category	Digital Services and Cyber Security
Policy scope	Organisation Wide
Version Date	2025
Implementation/Approval Date	May 2025
Review Date	June 2026
Review Body	Assistant Director - DTS

1. TABLE OF CONTENTS

1. INTRODUCTION

The importance of robust cyber resilience and information governance cannot be overstated and the need to protect sensitive information and ensure the continuity of business processes is paramount.

SYMCA is committed to fostering a culture of security awareness and continuous improvement. We encourage all stakeholders to familiarise themselves with the contents of this standard and to actively participate in its implementation.

By working together, we can build a resilient and secure digital environment that supports our organisation's mission and objectives.

1.1 PURPOSE

The purpose of this standard establishes guidelines to ensure the confidentiality, integrity and availability of sensitive information held by SYMCA is protected and secure.

This standard applies to all the computer systems or information resources used in relation to SYMCA's operations, whether the computer and information resources are wholly owned and operated by SYMCA or externalised through outsourcing, external suppliers or joint ventures.

Where third parties cannot fully comply with this policy, SYMCA will enforce contractual obligations to mitigate risks. Where compliance with the standard cannot be achieved by a 3rd party additional measures may need to be considered to protect data.

A. KEY DEFINITIONS

USER

A user is an individual who has access to and/or uses technology and/or information resources to provide services or products. This includes, but it is not limited to

- Individuals employed directly by SYMCA.
- Individuals employed by a company subcontracted by SYMCA to provide services to SYMCA.
- Individuals employed by a third-party providing services to SYMCA.

AUTHORISED PERSON

An authorised person is an individual who has been granted specific permissions, privileges, or rights to access, use or manage certain information and/or technology resources or systems within SYMCA.

1.2 ENFORCEMENT

Non-compliance with this standard may result in disciplinary action, including but not limited to account suspension or termination.

1.3 REVIEW

This policy will be reviewed annually. However, where gaps are found in existing policies, procedures, technologies, or security controls they will be corrected in a timely manner.

- This policy will be reviewed annually by the Information Governance Working Group in consultation with the SIRO.

2. PRINCIPLES

2.1 GENERAL PRINCIPLES

Information security protects the information that is entrusted to us. Failing to secure information can result in financial, legal, and reputational risks to SYMCA and its stakeholders. By having an effective information security management system, we can:

- Provide assurances for our legal, regulatory, and contractual obligations.
- Ensure the right people, have the right access to the right data at the right time.
- Provide protection of personal data as defined by the GDPR.
- Be good data citizens and custodians.

2.2 INFORMATION SECURITY OBJECTIVES

- To ensure the confidentiality, integrity and availability of organisation information including all personal data as defined by the GDPR based on good risk management, legal regulatory and contractual obligations, and business need.
- To provide the resources required to develop, implement, and continually improve the Information Security Management System.
- To effectively manage third party suppliers who process, store, or transmit information to reduce and manage information security risks.
- To implement a culture of information security and data protection through effective training and awareness.

2.3 INFORMATION SECURITY DEFINITION

Information security is defined as preserving:

a. **CONFIDENTIALITY: Access** to information shall be confined to those with appropriate authority.

b. **INTEGRITY: Information** shall be complete and accurate. All systems, assets and networks shall operate correctly, according to specification.

c. **AVAILABILITY:** Information shall be available and delivered to the right person, at the time when it is needed.

3. ROLES AND RESPONSIBILITIES

Information security is the responsibility of everyone to understand and adhere to SYMCA policies, follow process and report suspected or actual data breaches.

Specific roles and responsibilities for the running of the information security management system are defined and recorded in the document as follows:

CHIEF EXECUTIVE

Responsibility for information security resides ultimately with the Chief Executive. This responsibility is discharged through the designated roles of Senior Information Risk Owner (SIRO).

Responsible for overall governance and ensuring appropriate resourcing for security initiatives.

DATA PROTECTION OFFICER (DPO)

The primary role of the data protection officer (DPO) is to ensure that their organisation processes personal data in compliance with the GDPR and Data Protection.

SENIOR INFORMATION RISK OWNER (SIRO)

The Senior Information Risk Owner (SIRO) Ensures that SYMCA's risk management framework is embedded into all information security processes and reports directly to the CEO on security risks.

INFORMATION ASSET OWNERS (IAO)

Information Asset Owners (IAOs) are responsible for managing information risk and providing assurances to the SIRO. IAOs are typically Heads of Service or Assistant Directors and have responsibility for ensuring that the Information Asset Register is kept up to date and accurate.

4. DOCUMENT CONTROL

Version	Date	Brief Summary of Changes	Author
1.1	23/09/24	1st draft	Christine Marriott
1.2	11/03/2025	Updates throughout the document	Nick Brailsford
1.3	06/05/25	Read through and sign off	Nick Brailsford
2			
3			
4			
5			