

ONESOURCE INFORMATION SECURITY POLICY

Introduction

OneSource Specialty Pharma Limited (“OneSource” or “the Company” or “We”) is a pure-play specialty pharmaceutical CDMO with integrated capabilities across biologics, drug-device combinations, sterile injectables, and oral technologies. With over three decades of experience in specialised drug development and manufacturing, we support our partners from early-stage development through commercialisation, delivering high-quality, innovative, and reliable healthcare solutions.

We are committed to protecting the confidentiality, integrity, and availability of information entrusted to us. Accordingly, we maintain a governance framework designed to safeguard business information, intellectual property, technology systems, and other information assets. This framework supports the management of evolving security threats, regulatory and contractual compliance, business resilience, and the protection of stakeholder interests. This Information Security Policy (“Policy”) sets out the principles and responsibilities for managing information security risks across the Company’s operations.

Objective

The objective of this Policy is to establish OneSource's overarching principles for:

- protecting information and information systems against unauthorised access, use, disclosure, alteration, loss, or destruction;
- maintaining the integrity and availability of information required for business operations;
- identifying, monitoring, and responding to information security threats and incidents;
- establishing individual responsibilities for information security across the workforce;
- defining proportionate information security requirements for suppliers, contractors, service providers, and other relevant third parties; and
- supporting the continual improvement of the Company's information security framework.

Scope

This Policy applies to all employees, including permanent, temporary, contract staff, as well as suppliers and relevant third parties who access, process, store, or transmit, or manage OneSource information or information systems. It covers information in electronic, physical and other forms, and applies to information systems, applications, networks, devices and services used for OneSource business purposes.

Information Security Principles

Risk Management and Continuous Improvement

Information security risks are identified, assessed and managed using a risk-based approach that considers relevant threats, vulnerabilities, business impacts and existing controls. OneSource periodically reviews its information security framework and enhances controls and practices, as appropriate, to address changes in risks, business requirements, technology and applicable obligations.

Information Protection and Data Integrity

The Company applies appropriate administrative, technical and physical controls to protect information throughout its lifecycle. Information is handled in accordance with its sensitivity, criticality and applicable requirements. Access to information and systems is authorised based on business needs and the principles of least privilege and need-to-know and is reviewed and adjusted where appropriate.

Controls are maintained to support the accuracy, completeness, consistency and integrity of information and to protect information from unauthorised modification, disclosure, corruption, loss or destruction. Personal information is protected in accordance with applicable privacy and data protection requirements.

Security Monitoring and Threat Response

The Company monitors relevant information security risks and threats and maintains processes for the timely identification, reporting, assessment, containment, investigation, remediation and recovery of information security incidents. Suspected or confirmed incidents must be reported promptly through established channels.

Access, Systems and Technology Security

The Company maintains proportionate controls to protect information systems, networks, applications, devices and technology services. These controls may include identity and access management, secure configuration, vulnerability and patch management, malware protection, logging and monitoring, backup and recovery, and controls for mobile, remote and cloud-based working, as appropriate to the relevant risk and operating environment.

Workforce Responsibilities and Awareness

Information security is a shared responsibility across the workforce. Employees and other personnel within the scope of this Policy are expected to:

- handle information and use Company systems only for authorised business purposes;
- use only Company-authorised systems, accounts and communication channels for conducting Company business and handling Company information, and not use personal email accounts or other unauthorised channels for such purposes;
- protect passwords, credentials, devices and other information assets assigned to them;
- comply with applicable information security, privacy, acceptable-use and access-control requirements;
- complete information security awareness and training activities applicable to their roles;

- report suspected incidents, phishing attempts, security weaknesses or the loss of information or devices promptly; and
- continue to protect confidential information after a change in role or the end of employment or engagement.

Third-Party Information Security

The Company recognises that suppliers, contractors, and other third parties may have access to information and systems that support its operations. Accordingly, appropriate information security and data protection expectations are established for relevant third parties, taking into account the nature of the services provided and the associated risks. Information security requirements may be incorporated into relevant contractual arrangements to support the protection of OneSource information and systems.

Compliance

The Company identifies and addresses applicable legal, regulatory, statutory and contractual requirements relating to information security and data protection. Compliance with this Policy and related requirements may be reviewed through management oversight, risk assessments, audits or other assurance activities, as appropriate.

Governance Mechanism

The Company maintains a governance framework to provide appropriate oversight and accountability for information security. As part of this framework, the Risk Management Committee (“Committee”), operating under the oversight of the Board of Directors, provides strategic oversight of information technology, cybersecurity, and data-related risks. The Committee’s responsibilities include ensuring adherence to this Policy, overseeing the implementation of information security strategies and initiatives, and monitoring the continued effectiveness of the Company’s information security practices.

Incident Reporting

All personnel must promptly report suspected or confirmed information security incidents, security weaknesses, unauthorised access, loss of information or devices, or other events that may affect the confidentiality, integrity or availability of OneSource information. Reports must be made through the incident reporting channels communicated internally by OneSource. Information security and IT-related incidents are reviewed through established governance mechanisms, with appropriate remediation actions and progress tracking to support timely resolution.

Periodic Review of Policy

The Company’s information security framework, including its controls, processes and procedures, shall be independently reviewed at least annually or following significant changes. Respective business heads shall be responsible for ensuring compliance with applicable information security policies and standards.

Version Control Sheet

Version Number	Date of Board Meeting	Remarks
V1	Approved and adopted in the Board Meeting held on July 24, 2026	Adopted in line with requirements of ESG parameters