STRIDES PHARMA SCIENCE LIMITED

Information Security Policy

(Abridged Version)

Strides

1. Introduction

Strides Pharma Science Limited ("Strides" or "the Company") is dedicated to establishing and sustaining a robust information security framework that protects its information assets across all areas of its global operations. The Company recognises that effective information security is essential to preserving the confidentiality, integrity and availability of critical business information, including patient data, research and manufacturing information, intellectual property and enterprise systems. By implementing comprehensive security controls and governance practices, Strides seeks to mitigate evolving cyber risks, support business resilience, ensure compliance with applicable legal and regulatory requirements, and maintain the confidence of patients, customers, business partners and employees. This Information Security Policy ("Policy") defines the Company's commitment, guiding principles and security requirements for protecting its information assets from internal and external threats.

2. Objective

The objective of this Policy is to protect the confidentiality, integrity and availability of Strides' information assets, including business data, digital systems, manufacturing and laboratory technology, and intellectual property, through the implementation of appropriate information security controls. The Policy aims to reduce the risk of unauthorised access, data breaches, cyber threats and other information security incidents that may compromise Company or stakeholder information.

3. Scope

This Policy applies to all employees, contractors, consultants, vendors and third parties who access, process or manage Strides' information systems, networks, applications or data, across all Strides locations, subsidiaries and affiliates globally. It covers information in electronic, physical and verbal form.

4. Policy Framework

4.1. Information Security and Data Protection

- **Data Classification**: Information is classified based on its sensitivity, business criticality and regulatory requirements, with appropriate information security controls applied in accordance with its classification.

- **Access Control**: Access to information, systems and applications is granted based on the principles of least privilege and need-to-know and is subject to periodic review. User access is authorised, monitored and revoked in a timely manner to prevent unauthorised access and to ensure that access rights remain appropriate to business responsibilities.

- **Encryption**: Sensitive and confidential information is protected through encryption during transmission, storage and, where applicable, processing to prevent unauthorised access or modification.

- **Backup and Recovery**: Critical information is backed up regularly, and recovery procedures are periodically tested to ensure the availability and integrity of information following a disruption or data loss. Backup media is protected against unauthorised access, loss or corruption, and recovery capabilities are maintained to support business continuity and operational resilience.

- **Data loss monitoring**: Data Loss Prevention (DLP) controls are implemented to monitor, detect, and prevent unauthorized access, disclosure, or transfer of sensitive information across endpoints, networks, email, and cloud environments.

- **Data Integrity Protection:** Controls are implemented to ensure the accuracy, completeness, consistency, and integrity of information throughout its lifecycle and to prevent unauthorized modification, corruption, or destruction of data.

- **Email Security and Filtering**: Email security controls are implemented to detect and prevent phishing, malware, spam, spoofing, business email compromise (BEC), and other email-based threats. Security mechanisms such as email filtering, anti-phishing protection, and domain authentication controls are used to enhance email security and reduce the risk of cyber threats.

- **Web Security Monitoring and Protection**: Web security controls are deployed to monitor and block malicious websites, unsafe browsing activities, phishing sites, and other web-based threats. Web filtering and threat intelligence mechanisms are used to protect users from online risks and prevent unauthorized access to malicious content.

4.2. Security Monitoring and Threat Detection

- 24x7 Monitoring: A 24×7 Security Operations Centre (SOC) continuously monitors the organization's IT and OT environments using a Security Information and Event Management (SIEM) platform to detect, analyse, and respond to potential security incidents, unauthorized access attempts, and suspicious activities in real time.

- Threat Intelligence: The SIEM is integrated with threat intelligence feeds to enrich security events with contextual information, proactively identify emerging threats and indicators of compromise (IOCs), and enable timely detection and mitigation of evolving cyber risks.

- Centralised Log Management: The SIEM platform centrally collects, normalizes, correlates, and retains security logs from endpoints, servers, network devices, security appliances, cloud services, and critical applications. Log retention is maintained in accordance with applicable regulatory, legal, and compliance requirements to support continuous monitoring, forensic investigations, and audit readiness.

4.3. Network and System Security

- **Perimeter Defence:** Firewalls and intrusion prevention systems protect the network perimeter from unauthorised access and network-based attacks.

- **Patch Management:** Systems, applications and endpoints are kept current through structured patching to remediate known vulnerabilities.

- **Endpoint Protection:** Extended Detection and Response (XDR) solutions are deployed across servers and end-user devices to provide comprehensive threat detection, investigation, and response capabilities.

- **Network Segmentation:** Network segmentation is implemented across enterprise, manufacturing, and OT environments through the use of VLANs and VDOMs to restrict lateral movement and minimize the impact of potential security incidents.

4.4. Incident Response and Business Continuity

- **Incident Response Plan:** A documented Incident Response Plan is established and maintained to define structured procedures for the identification, containment, eradication, and recovery of security incidents. The plan ensures effective coordination, timely response, and restoration of affected services during cybersecurity events.

- **Incident Reporting and Security Awareness:** All personnel are required to promptly report suspected or confirmed cybersecurity incidents to the designated security team through established reporting channels. Regular cybersecurity awareness training is provided to employees to enhance their ability to recognize cyber threats, identify potential security incidents, and follow appropriate reporting and escalation procedures.

- **Disaster Recovery and Business Continuity:** Disaster Recovery (DR) plans are established, maintained, and periodically tested to validate the organization's ability to restore critical systems and services within defined recovery objectives, ensuring business continuity during disruptive events.

- **Forensics and Lessons Learned:** Significant security incidents are subject to detailed forensic analysis to determine the root cause, assess the impact, and identify improvement opportunities. Lessons learned from incident investigations are documented and used to enhance security controls, update response procedures, and strengthen the organization's overall cybersecurity resilience.

4.5. Vulnerability and Risk Management

- **Vulnerability Assessments:** Regular vulnerability assessments and penetration testing are conducted across systems, applications and infrastructure.
- **Risk-Based Remediation:** Identified vulnerabilities are prioritised by risk and remediated through structured patch and change management processes.

4.6. Employee Awareness and Training

- **Security Awareness and Mandatory Training:** All employees are required to complete periodic information security awareness training as part of the organization's cybersecurity program. The training covers key security topics, including phishing awareness, social engineering, password hygiene, safe data handling practices, secure use of company resources, incident reporting procedures, and protection against emerging cyber threats. Training completion is monitored to ensure all personnel maintain awareness of their security responsibilities.

- **Phishing Simulation and Awareness Testing:** Periodic phishing simulations and security awareness assessments are conducted to evaluate employee readiness, reinforce secure behaviours, and improve resilience against phishing, social engineering, and other cyberattack techniques.

- **Information Security Responsibilities:** All employees, contractors, consultants, and temporary personnel are responsible for protecting Strides' information assets and complying with applicable information security requirements, policies, standards, and procedures. Personnel must exercise due care when handling information, protect credentials and devices, report suspected security incidents promptly, and actively support the organization's cybersecurity objectives.

4.7. Data Privacy

Strides is committed to protecting personal data in accordance with applicable data protection and privacy laws, including those governing patient, employee and business partner information. Personal data is processed lawfully, used only for defined business purposes, and protected through appropriate technical and organisational measures.

4.8. Compliance and Regulatory Requirements

- **Regulatory Alignment:** Strides comply with applicable laws, regulations and industry standards relating to information security and data protection across the jurisdictions in which it operates.

- **Audits and Assessments:** Independent and internal security audits are conducted periodically to evaluate the effectiveness of controls and identify areas for improvement.

- **Continuous Improvement:** Strides is committed to the continual improvement of its information security management framework. Information security controls, technologies, processes, and governance mechanisms are periodically reviewed and enhanced to address evolving cyber threats, business requirements, emerging technologies, regulatory developments, and lessons learned from security incidents and assessments.

Strides

4.9. Third Party Information Security

- **Third-Party Security Requirements:** Suppliers, contractors, service providers, and other third parties that access, process, store, transmit, or manage Strides information or information systems are expected to comply with applicable information security and data protection requirements established by Strides. Third parties are also expected to adhere to the principles and requirements set forth in the Strides Vendor Code of Conduct, including maintaining appropriate controls to protect confidential information, implementing adequate risk management and business continuity measures, complying with applicable laws and regulations, and reporting actual or suspected security incidents that may impact Strides. Compliance with these requirements shall be assessed through contractual obligations, due diligence, and ongoing vendor governance processes.

- **Security Due Diligence:** Information security risks associated with third parties are assessed as part of vendor onboarding, contracting, and periodic review processes.

- **Contractual Security Obligations:** Appropriate information security, confidentiality, privacy, and incident notification requirements shall be incorporated into relevant contractual agreements with third parties based on the nature of services provided and associated risk levels.

- **Monitoring:** Critical third-party providers may be subject to periodic security assessments, audits, attestations, or other assurance activities to validate compliance with applicable information security requirements.

This version presents the key elements of the detailed operational policy in an abbreviated format.

*****