HUDEVAD
RADIATOR DESIGN

Information Security Policy

Contents

1. Introduction

We are committed to ensuring that we manage information securely. We take the responsibility of being entrusted with our stakeholders' personal data very seriously and we are committed to protecting all data with the highest levels of security.

Furthermore, information security is critical to the sustainability and competitiveness of our business, as well as being part of our responsibility to our customers, colleagues, suppliers, contractors and investors.

2. Purpose

The purpose of this policy is to establish a framework for protecting the confidentiality, integrity, and availability of information assets owned or processed by Stelrad Group plc and its subsidiaries ("the Group").

3. Scope

The Information Security Policy and its supporting controls, processes and procedures apply to all information used by the Group, in all formats. This includes information processed by other organisations in their dealings with the Group.

The Information Security Policy and its supporting controls, processes and procedures apply to all individuals who have access to Group information and information systems or services. This includes all colleagues, suppliers, contractors and company partners who are given access to Group information. This also includes external parties that provide information processing services to the Group.

4. Principles and Objectives

It is the Group's policy to ensure that information is protected from a loss of:

- confidentiality – information will be accessible only to authorised individuals and we take the highest level of care in protecting information
- integrity – our robust systems and processes ensure that the accuracy and completeness of information will be maintained
- availability – information will be accessible to authorised users and processes at the time they are needed.

As such, the Group's security objectives are that:

- our information risks are identified, managed and treated according to an agreed risk tolerance
- our authorised users can securely access and share information in order to perform their roles
- our physical, procedural and technical controls balance user experience and security
- our contractual and legal obligations relating to information security are met
- information security is considered across all the Group's activities and businesses
- individuals accessing our information are aware of their information security responsibilities

5. Governance and responsibility for information security

Accountability for Information Security sits with the Chief Financial Officer who reports directly to the Group Board.

In addition, the Board and Executive Directors receive detailed updates on our risk management and mitigation activities through the Group's Audit & Risk Committee.

An Information Security steering group influences, oversees and promotes the effective management of Group information and communicates developments in information risk to the Chief Financial Officer.

6. Information security policies and risk management

To deliver and demonstrate our commitment, we have developed policies that set out our ambition and have implemented controls to prevent, detect and mitigate risks. We have adopted a risk-based approach which is used in prioritising activities on those areas that are highest risk to the business.

We have also established reporting processes and an Information Security steering group to raise visibility with leadership teams and across the Group. Information risk registers and information assets registers are reviewed within the Information Security steering group. We continuously invite challenge through independent information security reviews and audits.

7. Systems Security

In order to ensure our technology systems are protected against changing security vulnerabilities, we regularly test and install 'patches'.

In addition, we continue to strengthen our network to help us protect against unauthorised traffic and malicious content entering our environment. We have deployed tools to protect us against malware infections.

We have independent penetration testing performed annually to actively identify vulnerabilities.

Systems and applications that are developed are scrutinised for security bugs and weaknesses throughout their development before being launched. And our information security infrastructure is subject to comprehensive monitoring.

We have a process in place for the identification and escalation of security incidents.
Actual or suspected breaches of information security are recorded and investigated. The appropriate action to correct the breach will be taken, and any learning built into controls.

8. Employee awareness training

We make sure that our employees are trained in security awareness so that they understand the importance of confidentiality, integrity and availability and their responsibility to preserve it. On-going training is also undertaken to help further protect our customer, employee and business information.

Employee information security awareness training is mandatory. We deliver regular refresher training to ensure it remains current in everyone's minds.

9. Supplier relationships and supplier audit

We expect our suppliers to take the same level of care as we do for the information shared with them. The Group's information security requirements are considered when establishing relationships with suppliers, to ensure that assets accessible to suppliers are protected.

Supplier activity is monitored and audited according to the value of the assets and the associated risks.

10. Business Continuity

To maintain the successful ongoing operation of our business, we regularly conduct business impact assessments on our functions to identify capabilities, needs and criticalities to our business. We then implement response plans, controls and mitigations to help protect those essential processes. Business continuity plans are maintained, reviewed and tested regularly.

We also have appropriate backup routines and built-in resilience in our IT systems which we test regularly.

11. Cyber risk management

Each of the Group's business units will implement the following procedures to manage cyber risk:
- Conduct regular vulnerability assessments and penetration tests.
- Implement a security awareness training program for all employees.
- Use strong passwords and multi-factor authentication.
- Implement a data backup and recovery plan.
- Have a plan for responding to cyber incidents.

In the event of a cyber incident, the Group will take the following steps:
- Immediately investigate the incident.
- Contain the incident and prevent further damage in conjunction with the SOC.
- Restore any lost or damaged data.
- Report the incident to the appropriate authorities.
- Communicate with affected parties.

The Group will comply with all applicable laws and regulations related to cyber security.

12. Compliance

The design, operation, use and management of our information systems complies with all statutory, regulatory and contractual security requirements, including:

- data protection legislation - If personal data is transferred it must comply with the requirements of the General Data Protection Regulation (GDPR), where applicable
- the payment card industry standard (PCI-DSS) - If a third party is processing card payments it must comply with Payment Card Industry Data Security Standard (PCI DSS), where applicable
- The Group's contractual commitments

We use a combination of internal and external audits to demonstrate compliance against chosen standards and best practice, including against internal policies and procedures, including IT health checks, gap analyses against documented standards and internal checks on employee compliance.

We encourage anyone concerned about wrongdoing in contravention of any aspect of this policy to speak up by contacting a line manager, HR contact or raising their concerns using the Group whistleblowing policy (the contact details are: compliance@srgl.com or +44 191 261 3306).

Policy review

A review of this policy will be undertaken by the Group Finance Department and will be approved by the Board.

.

Responsibility for document:	Group Finance Department
Effective date:	October 2023
Frequency of review:	Every two years
Next review date:	October 2025

Version control

Date	Version	Reason for change	Author
October 2023	1.0	Initial release	Group Finance Department