INFORMATION SECURITY POLICY

Purpose

Information collected, analysed, stored, communicated, and reported upon may be at risk of theft, misuse, loss, or corruption. Inadequate education and training and a breach of security controls can also put information in danger.

Information security incidents can cause harm to the company, including embarrassment, financial loss, failure to comply with standards and regulations, and potential legal repercussions.

This high-level Information Security Policy works alongside the 'Information Risk Management Policy' and 'Data Protection Policy.' Its purpose is to provide an outline of Revvence's risk-based information security controls and explain why they are necessary.

Objectives

Revvence's security objectives are the following:

- our information risks are identified, managed and treated according to an agreed risk tolerance
- our authorised users can securely access and share information 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
- our teaching, research and administrative activity consider information security
- individuals accessing our information are aware of their information security responsibilities
- incidents affecting our information assets are resolved and learnt from to improve our controls

Scope

The Information Security Policy and its accompanying controls, processes, and procedures apply to all information utilised at Revvence, regardless of its format. This includes information handled by other organisations while dealing with Revvence.

Moreover, the Information Security Policy and its supporting controls, processes, and procedures apply to all individuals with access to Revvence's information and technologies, including external parties providing information processing services to Revvence.

Compliance Monitoring

An information security team will monitor compliance with the controls in this policy and report to the Board.

Review

The information security team will review this policy annually or as required and will have it approved by the Board of Directors.

Policy Statement

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

- confidentiality – information will be accessible only to authorised individuals
- integrity – the accuracy and completeness of information will be maintained
- availability – information will be accessible to authorised users and processes when required

Revvence will implement an Information Security Management System based on certified standards applicable to the business.

Revvence will adopt a risk-based approach to the application of the following controls:

Information security policies

To support the high-level Information Security Policy and its objectives, a set of lower-level controls, processes, and procedures will be defined. This suite of supporting documentation will be approved by the Board, published, and communicated to Revvence users and relevant external parties.

Organisation of information security

Revvence will establish appropriate governance arrangements to manage information security, which will involve assigning and delegating security responsibilities to initiate and control the implementation and operation of information security within Revvence.

Revvence will appoint the following roles:

- an Executive to chair an Information Governance Board and take accountability for information risk
- an Information Governance Board to influence, oversee and promote the effective management of Revvence information
- an Information Security specialist to manage the day-to-day information security function

Human resources security

Revvence will ensure that all its users know its security policies and expectations regarding acceptable use. The company will provide information security education and training to its users so that they understand their responsibilities. The company will address any inappropriate or poor behaviory. Additionally, when appropriate, security responsibilities will be included in role descriptions and personal development plans.

Asset management

All assets will be documented and accounted for. This may include:

- information
- software
- electronic information processing equipment
- service utilities
- people

When deemed necessary, every asset will have an owner designated and held accountable for maintaining and safeguarding it. All information assets will be categorised according to their legal obligations, business importance, significance, and vulnerability. This classification will indicate the necessary handling requirements. Furthermore, each information asset will have a pre-defined schedule for retention and disposal.

Access control

Access to all information will be controlled and managed based on business requirements. Users will be given access, or arrangements will be made according to their role and information classification. Access will be granted only to the level necessary to perform their duties.

A formal user registration and de-registration procedure will be maintained for access to all information systems and services. This will include mandatory authentication methods based on the sensitivity of the information being accessed and consideration of multiple factors as appropriate.

Specific controls will be implemented for users with elevated privileges to reduce the risk of negligent or intentional system misuse. Where practical, the separation of duties will be implemented.

Cryptography

Revvence will provide guidance and tools to ensure the proper and effective use of cryptography to protect information and systems' confidentiality, authenticity and integrity.

Physical and environmental security

When necessary, Revvence will store its information processing facilities in secure areas that are physically protected from unauthorised access, damage, and interference. We will have layered internal and external security controls to prevent unauthorised access and protect our assets, including critical or sensitive ones, against hidden or forcible attacks.

Most of Revvence's information processing systems are managed by third-party providers like Google and Oracle. We will ensure that these third-party providers have proper access controls in place.

Operations Security

Revvence will ensure the correct and secure operations of information processing systems. This will include:

- documented operating procedures
- the use of formal change and capacity management
- controls against malware
- defined use of logging
- vulnerability management

Communications Security

Revvence will ensure the security of its networks to protect the information stored within them, as required. It will also provide guidance and tools for safely transferring this information, both within its networks and with external entities. This will be following the classification and handling requirements associated with the particular information.

System Acquisition, Development and Maintenance

Information security requirements will be determined when developing new information systems or changing existing ones. Appropriate controls will be implemented to mitigate any identified risks. Additionally, all system development will implement change control and separation of test, development, and operational environments.

Supplier relationships

Revvence's information security requirements will be considered when establishing relationships with suppliers to ensure that assets accessible to suppliers are protected.

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

Information Security Incident Management

There will be instructions on what qualifies as an information security incident and how to report it. Any actual or suspected information security breaches must be reported and thoroughly investigated. The necessary steps will be taken to rectify the breach, and any lessons learned will be incorporated into our security controls.

Information Security Aspects of Business Continuity Management

Revvence will implement measures to safeguard critical business processes against the repercussions of major information system failures or disasters. The objective is to ensure that these processes are promptly restored following predetermined business requirements. The measures will involve suitable backup procedures and resilient design.

Business continuity plans must be regularly reviewed and tested to support this policy. A business impact analysis will also be conducted to outline the potential consequences of:

- Disasters
- security failures
- loss of service
- lack of service availability

Compliance

The operation, use, design, and management of information systems must comply with all applicable statutory, regulatory, and contractual security requirements.

Currently, this includes:

- data protection legislation
- Revvence's contractual commitments
- ISO27001 (aspirational)

Revvence will use a combination of internal and external audits to demonstrate compliance against chosen standards and best practices, including internal policies and procedures. This will include:

- IT health checks
- gap analyses against documented standards
- internal checks on staff compliance

Review of this document: annually by: Chair of the Information Governance Board

Next review date: April 2025.