

<i>Document Title</i> Information Security Management Policy	<i>Approved by</i> Martin Carlesund, CEO	<i>Entry Into Force Date</i> November 1 st , 2022	<i>Company</i> Evolution AB (publ)	
<i>Owner</i> Information Security department	David Craelius, CTO	<i>Last Review Date</i> July 18 th , 2024	<i>Security Class</i> Internal	<i>Version</i> 3.0
<i>Scope</i> Global	Julia Simonsson, CLO			

EVOLUTION GROUP POLICY

INFORMATION SECURITY MANAGEMENT POLICY

Contents

- 1. Purpose and Scope..... 3
- 2. Policy Statement..... 3
- 3. Information Security Principles 4
- 4. Supporting and Advancing Policies 4
- 5. Policy Objectives..... 4
- 6. Roles and Responsibilities..... 6
- 7. Bypassing or Breaching Security Measure..... 7
- 8. Information Security Risk Management..... 7
- 9. Physical Security 8
- 10. Password Policy 8
- 11. Clean Desk and Desktop Policy 9
- 12. Policy Exemptions..... 9
- 13. Security and Privacy Events and Incidents10

1. Purpose and Scope

This information Security Management Policy ("Policy") has been established to communicate the intent of implementing information security throughout the business, to provide clear direction and support to all internal and external stakeholders, to establish a security conscious culture and to provide the mandate to address information security risks throughout the Evolution AB ("Evolution", or the "Company" and together with its subsidiaries the "Group").

The scope of this Policy includes but is not limited to the implementation of managed security services for all Evolution's information systems and assets; both physical and intellectual located in all Evolution's locations and impacts all entities, including permanent and temporary employees. Contractors and third party or outsourced service providers; considering all legal and regulatory requirements and constraints.

This Information Security Management Policy:

- Applies to all staff, consultants, contractors, partnership organizations and partner staff of Evolution.
- Covers all information handled, in any format, stored, processed, or shared by Evolution, irrespective of whether that information originates with or is owned by Evolution.
- Applies to all computer and non-computer-based information systems owned by Evolution, or used for Evolution's business, or connected to Evolution's managed networks.

Evolution is certified against ISO/IEC 27001:2013 standard and forms the Information Security Management System (ISMS) framework. - systematic approach consisting of processes, technology and people that helps protect and manage Evolution's information through effective risk management.

Scope of ISMS: Software development. Solutions development. Provision, maintenance, and servicing of product platform. IT solutions and provision of direct Gaming studio transmission services.

2. Policy Statement

Evolution recognizes the importance of Information Security to protect all assets of Evolution. Evolution management has identified the risks related to Information Security and defined a framework for the management, which provides the mechanism for security control integration, and management.

Evolution is committed to a robust implementation of Information Security Management. It aims to ensure the appropriate confidentiality, integrity and availability of its data and other assets. The principles defined in this Policy are applied to all the physical and electronic information assets for which the Group is responsible.

3. Information Security Principles

Information security follows four overarching principles:

Confidentiality: This means that information is only being seen or used by people who are authorized and have the necessity to access it for job duties based on need to know.

Integrity: This means that any changes to the information by an unauthorized user are impossible (or at least detected) and changes by authorized users are tracked.

Availability: The information is accessible when authorized users need it wherever they are. Availability is protected by implementing appropriate controls that ensures it.

Usability: Implemented tools, policies and standards need to support business.

4. Supporting and Advancing Policies

Information Security Management System is formed by this Policy and its supporting and advancing policies.

Group supporting policies:

- Data protection and privacy Policy
- Whistleblowing Policy
- Risk Assessment Policy

Policies advancing from this Policy:

- Patch and vulnerability management policy
- Record Retention & Destruction policy
- Information classification & Asset management policy
- Change management policy
- Access management policy
- Encryption key management policy
- Physical security standard
- Password policy
- Clean desk policy

The list of advancing policies might be extended to cover the requirements of the implementation of the Information Security Management System.

5. Policy Objectives

Evolution has identified a set of objectives, which forms the basis of Information Security Management policies and supporting and advancing policies within Evolution. They are as follows:

- To provide management direction and support for information security in accordance with business requirements and current regulatory requirements
- To manage information security within the organization
- To maintain the security of Evolution's information and information processing facilities that are accessed, processed, communicated to, or managed by internal and external parties
- To achieve and maintain appropriate protection of Evolution's assets
- To ensure that information receives an appropriate level of protection
- To ensure employees, contractors and third-party users understand their responsibilities and are suitable for the roles they are considered for to reduce risk of theft, fraud, or misuse of facilities; are aware of information security threats and concerns, their responsibilities, and liabilities, and are equipped to support security in the course of their normal work and to reduce the risk of human error and to ensure their exit from Evolution is conducted in a timely and orderly manner
- To prevent unauthorized physical access, damage and interference to Evolution's premises and information
- To prevent the loss, damage, theft or compromise of assets and interruption to Evolution's activities
- To ensure the correct and secure operation of information processing facilities
- To implement and maintain the appropriate level of information security and service delivery in line with third party service delivery agreements
- To minimize the risk of system failures
- To protect the integrity of software and information
- To ensure the protection of information in networks and the protection of the supporting infrastructure
- To prevent unauthorized disclosure, modification, removal or destruction of assets and interruption to business activities
- To maintain the security of information and software exchanged within the Evolution Group and with any external entity
- To detect unauthorized information processing activities
- To control access to information, managing authorized user access and to prevent unauthorized access to information systems, preventing unauthorized user access and compromise or theft of information and information processing facilities, preventing any unauthorized access to networked services and access to operating systems or any information held on application systems
- To ensure information security when using mobile computing facilities
- To ensure security as an integral part of information systems
- To prevent errors, loss, unauthorized modification, or misuse of information in applications

- To protect the confidentiality, authenticity, or integrity of information by cryptographic means
- To ensure the security of system files
- To maintain security of application system software and information
- To reduce risks resulting from exploitation of published technical vulnerabilities
- To ensure information security events and weaknesses associated with information systems are communicated in a manner allowing timely corrective action to be taken
- To ensure a consistent and effective approach is applied to the management of information security incidents
- To counteract interruptions to business activities and to protect critical business processes from the effects of major failures of information systems or disasters and to ensure their timely resumption
- To avoid breaches of any law, statutory, regulatory, or contractual obligations and of any security requirements
- To ensure compliance of systems with organizational security policies and standards
- To maximize the effectiveness of and to minimize interference to/from the information systems audit processes.

6.Roles and Responsibilities

Employees are responsible for:

- Adhering to this Policy and all related policies, processes, and procedures
- Getting consulted by Manager or Information Security team when unsure how to comply with this Policy
- Reporting security incidents, breaches, alerts, or similar instances to the Information Security team and / or Data Protection team.

The Information Security Department and Head of Security has overall responsibility for:

- the development and upkeep of this Policy
- ensuring this Policy is supported with appropriate documentation
- ensuring that all documentation is relevant and current
- ensuring this Policy is communicated to all departments and employees.

The Information Security Department has specific and overarching responsibilities for preserving the confidentiality, integrity, and availability of information.

This Policy, together with all supporting policies and procedures forming the Information Security Management System, will be audited annually and changes will be authorized by the CEO.

All advancing policies shall be approved by Group CTO.

Audited results and changes will be documented and stored in a central location. All documents must be made available for review by relevant regulatory authorities.

7. Bypassing or Breaching Security Measure

Evolution has a set of controls in place to treat information security risks by mitigating, decreasing, accepting, escrowing risks.

Controls such as access management both physical and virtual, confidentiality offense or malicious. Security measures, such as a firewall, access controls and intrusion detection systems, have been put in place to protect Evolution from breaches that originate from outside sources. Any activity that bypasses or is intended to bypass or disable the security measures that are in place to protect Evolution networks contravenes the Policy.

Disregarding this Policy and related policies may be a subject for information security incidents. Additionally, failure or violation of the Policy may result in disciplinary action for employees, including termination from employment, or legal action (civil penalties and/or criminal sanctions, depending on the circumstances).

8. Information Security Risk Management

Taking an action or doing regular procedures we are subject to risks that can impact our work and leave a negative effect. It is important that we manage risks so that the negative impact of risks upon achievement of our objectives is minimized and our ability to realize potential opportunities is maximized. It is important in a day-to-day job to identify risks and make a proper decision on them.

The objective of Risk Management is to identify and value potential negative events to better handle or reduce the negative impact of an event or the probability of a negative event occurring. Risk assessment process is applied to protect information security, to safeguard it by identifying risks that are associated with the loss of confidentiality, integrity, and availability for information within scope of Information Security Management System (ISMS).

Each employee is responsible to stay aware and take into consideration potential threats to information security in daily operations. If a potential threat is identified, it should be reported to the direct manager or Information Security to investigate.

The Risk Owners are responsible for the risk assessment process, identification of threats and vulnerabilities. Usually, risk owners are senior managers within their division that take overall responsibility of Company assets.

It is important that Employees stay aware and thoughtful of information security in every day-to-day operation or when starting new projects or processes. Any new information system, or

infrastructure components as well as new processes should be assessed against potential threats to Information Security that the new process or planned item might affect.

Additionally in cases where new projects or systems include personal data, an assessment towards privacy risks should be made to prevent harm to a person's privacy. Data protection team can assist and consult to help implement new processes and projects in an appropriate manner.

Information Security risk management is subject to Evolution Group Policy: [Evolution Group Risk Assessment Policy](#).

9. Physical Security

All Evolution employees, contractors and third parties who are on Evolution premises remain accountable for actions under physical security requirements.

All employees must ensure they remain observant, report suspicious behaviour, and highlight non-compliance. This will help deter, delay, prevent and/or detect unauthorized access to, or attack on, a location and mitigate the impact should they occur.

More detailed explanation and precise requirements for physical security are detailed in following documents: [Physical Security Standard](#).

Employees must refer to these documents for detailed principles and procedures. It is also responsibility that requirements in these documents are applicable to 3rd parties and visitors, etc.

10. Password Policy

To protect Company assets and to prove authorized access, a secure logon procedure must exist for all critical information systems. Each user is responsible for the security token received such as password.

Full password policy is available here: [Password Policy](#).

All Users shall abide to minimum password requirements:

- Users must not write down their password and must not disclose their password.
- Not a single individual in Evolution will ask for a user password – **under no circumstances should the individual logon or password be shared**. The sharing of passwords is considered a serious disciplinary offense and will be dealt with accordingly.
- Users must think of a password that **is not** easily guessed by others, for example.

- The following are not suitable – dictionary words, car makes, telephone & room numbers; forenames and surnames; common words e.g., colours, seasons, days, sports, beverages etc.; simple keyboard sequences e.g., qwerty; words associated with computers.
- Users must ensure their Evolution login password is different from any other passwords they use to access non-Evolution systems or devices.
- System level passwords (e.g., Root, Administrator, Service Accounts) must be stored in an approved encrypted password vault provided by Evolution.
- As soon a password is compromised it should be changed immediately and the Evolution Information Security team must be informed. (security@evolution.com and / or Jira INFOSEC project).
- All users are responsible for reporting any suspected misuse of passwords to the Evolution Security department (security@evolution.com and/or Jira INFOSEC project).

Application owners, developers and / or administrators must enforce password policy requirements. Responsible teams managing Company Information Systems shall consult with the Information Security team for how to configure secure logon procedures for applications and information systems in scope.

Information Security team or external auditor may perform password policy check on IS systems in scope. All findings non-compliant with password policy should without undue delay be resolved.

11. Clean Desk and Desktop Policy

Clean desk & desktop policy is to establish a culture of security and trust for all employees at Evolution. An effective clean desk effort involving the participation and support of all Group employees greatly protects the sensitive information about employees, customers, and vendors from being exposed and / or stolen.

Aim is to reduce the threat of a security incident, as confidential information is locked away when unattended, hidden from sight, but additionally, clean desk policy implementation casts a positive image of the Group to employees and visitors.

12. Policy Exemptions

If there is a valid business reason for a user, a software installation, configuration, or a process to operate in contravention of the Policy, a request can be made to the Information Security team for an exemption. Request is submitted via User Support and must include part of the Policy where exception is necessary. The Information Security team will either approve or deny requests, in case of approval a specified time frame will be set. Permanent exemptions will not be granted.

13. Security and Privacy Events and Incidents

Information Security Event – An identifiable occurrence that has the potential to have an impact on information security. The event posed a risk to damage information security in terms of confidentiality, integrity, and availability, but did not.

Information Security Incident – An Information Security Event that resulted in:

- Damage to information assets
- A breach of Information Security rules; or
- Is considered a viable risk.

Privacy Events and Incidents – these are a subcategory of Information Security Incidents. They focus on incidents and events that impact systems storing personal information. The response to such incidents is conducted in accordance with established privacy frameworks.

Information Security incidents and events must be reported as soon as possible to the Information Security team through available communication channels such as:

- Direct manager
- Slack channel – #ask-security
- Email – security@evolution.com.

This includes any security event or suspected incident of malicious or illegal activity involving any corporate information or computing resources.

The Information Security department is responsible for overseeing any security incident response and investigation.

Controls and logging must be in place to log and monitor access to network and information assets to detect unauthorized access or malicious activity. The Information Security team is responsible for reviewing these logs on a regular basis to identify security incidents, including those relating to Policy non-compliance.

For non-regular and high impact information security incidents a root cause analysis shall be performed and registered, if necessary, appropriate changes shall be applied to decrease risk for the event to occur again.

All non-compliances or i.e., non-conformities that are to be identified due to the audits or following information security incident management process shall be registered and an action plan to fix them created.