Raiffeisen Bank International

# GROUP SECURITY

## TECHNICAL AND ORGANIZATIONAL MEASURES

# Content

# Introduction

Security has top priority for Raiffeisen Bank International. Data from customers and partners are treated with utmost care. To ensure trust in its professional services, RBI has implemented several technical and organizational measures. The rapid changes in technology and its open nature require constant adaptation and improvement of security measures from a technical as well as an organizational point of view. The attached document provides an overview of what is being done at RBI to protect information as well as technical infrastructure.

**Fundamental Principles of Security**

Security aims at providing confidentiality, integrity and availability of information. All technical and organizational measures at RBI are designed to protect these principles.

- Confidentiality means that information is not made available to unauthorized individuals, entities or processes.
- Integrity refers to accuracy and completeness of information.
- Availability means information being accessible and usable upon demand by an authorized entity.

**Security Framework**

In order to achieve the set goals, a framework is required to act as foundation for an efficient Security program. RBI's Security framework and its information security management system consist of the cornerstones identify, prevent, detect, respond and recover.

Since mid-April 2020 RBI Head Office has been officially certified according to ISO 27001:2013, the de facto standard for Information Security Management. Therefore, RBI has processes and procedures in place to adequately address and continuously improve Security in a structured way throughout the entire company.

**Strategic Approach to Security**

RBI constantly develops and adapts its Security strategy to actively identify, evaluate and minimize new threats and risks.

# Organizational Measures

Security is more than just a technical issue. People and processes must also be taken into consideration so as to adequately address Security company-wide.

**Security Policies:** A Security policy framework is defined. It reflects the need of a decentralized network of banking institutions and establishes modern standards in order to constantly improve and adapt the overall Security status.

**Security Risk Management:** Security risks are identified, assessed and prioritized for mitigation. Controls and mitigation plans are defined, implemented and tested.

**Contact to Authorities and Interest Groups:** RBI is in regular contact and closely cooperates with relevant authorities and interest groups to stay abreast of the latest trends and regulations in security.

**3rd Party Risk and Outsourcing Management:** Each external partner is assessed prior to commissioning by means of due diligence.

**Security Awareness:** Every employee must regularly attend or complete security awareness trainings or e-learnings, respectively.

**Professional Development:** Regular training is mandatory in order to stay up-to-date with modern technologies.

# Technical (Operational) Measures

**Information and Cyber Security**
To ensure trust in its professional services, RBI protects its business and customer data from unauthorized access, hacking attempts, malware infections, DDoS attacks, ATM fraud, data leakages, phishing attempts, disclosure of sensitive information and other threats with technical measures. Mitigation measures are implemented to ensure an appropriate risk level concerning confidentiality, integrity, availability and resilience of all systems.

**Cyber Threat Intelligence (CTI):** Internal and external specialists gain information about threats, analyze them and define security controls accordingly.

**Network Security:** Systems in networks are protected by technical and organizational measures: The networks are segmented and resilient, network access is protected, and traffic is analyzed and filtered.

**Cryptography:** Where appropriate, cryptographic measures are in place to ensure confidentiality of data and integrity.

**Device Security:** Devices are encrypted and centrally managed. Access to the corporate network is possible only via authorized devices.

**Anti-Malware and SPAM Protection:** Anti-malware services and systems are in use to detect, prevent and report (use of) malicious software and behavior.

**Access Control/Authentication and Authorization:** As a part of the user lifecycle management, defined processes for adding, changing and removing users and their access rights are applied. Access rights are provisioned according to need-to-know, need-to-have or need-to-do principles. Regular reviews of access rights are conducted.

**Password Security:** The complexity and length of passwords are set according to best practices and adapted if necessary.

**Secure Software Development:** Software is developed according to defined secure software development and secure coding practices based on leading industry standards.

**Security Tests:** Internet-facing systems as well as critical systems are penetration-tested by external, accredited, highly reputational security companies so as to further mitigate the risk of security software vulnerabilities.

**Data Classification:** RBI has implemented a classification model consisting of distinct levels which must be followed by all RBI employees. The protection level and requirements for data processing are defined for each classification category.

**Data Loss Prevention:** All devices are encrypted and the use of external media is restricted in order to prevent data loss or leakage through distribution channels. In addition, several measures are in place to detect and block connections to malicious or undesired websites and content.

**Data Masking (Anonymization):** Data in non-productive environments such as test and development environments is masked to prevent potential misuse.

**Vulnerability and Patch Management:** Both internal and external vulnerability scans are regularly performed to ensure that vulnerabilities are detected promptly and fixed based on their criticality.

**Security Monitoring:** Monitoring systems are in place to detect, analyze and react to anomalous activities indicating security incidents.

**Incident Management:** An incident management process is established so as to handle incidents in a timely manner. The main objective is to return to normal business as soon as possible.

**Business Continuity Management (BCM)**

BCM is a framework for identifying an organization's risk of exposure to internal and external threats. In RBI, the objective of BCM is to provide the ability to effectively respond to threats such as natural disasters or data breaches and protect the bank's business interests. The BCM lifecycle shows the stages of activity that must be gone through and repeats itself with the overall objective of improving organizational resilience.

| | |
|---|---|
| | **Policy and Program Management:** The Business Continuity policy provides the framework around which the BCM program is designed and built. It is the key document defining scope and governance. |
| | **Embedding Business Continuity:** Business Continuity is continually integrated into RBI's day-to-day business activities and organizational culture through training and education. |
| | **Analysis:** Objectives, processes and constraints of the environment in which RBI operates are reviewed and assessed. The main technique used is the Business Impact Analysis. |
| | **Design:** Appropriate strategies and tactics are identified and selected to determine how continuity and recovery from disruption can be achieved. |
| | **Implementation:** The agreed strategies and tactics are executed through the process of developing the Business Continuity Plan. |
| | **Validation:** Business Continuity Tests and Disaster Recovery Tests confirm that the BCM program meets the objectives set in the policy. |

**Physical Security**

Physical Security Management restricts physical access to RBI's premises in order to protect data and data systems with a mix of interacting organizational, constructional and technical measures in a layered defense approach.

**Security Zoning:** Premises are categorized in various protection zones.
A zone's security level depends on the criticality of assets in it.

**Access Control Management and System:** An access control system is used to grant and trace access to the protection zones as well as maintain access permissions.

**Security Personnel:** Security staff is employed to detect or ward off problems at the earliest possible stage and also acts as response team in the monitoring center.

**Intruder Alarm System:** An intruder alarm system is used to detect unauthorized entry into any protection zones.

**Video Surveillance:** Video surveillance supports security management in deterring, detecting and documenting unauthorized access and any kind of inappropriate or unlawful activities.

**Secure Disposal:** RBI enforces a secure waste management to securely eliminate sensitive data. Appropriate means are provided by external sources.