Rubin Data Security Policy

1. Purpose

Rubin must restrict access to confidential and sensitive data to protect it from being lost or compromised in order to avoid adversely impacting our customers, incurring penalties for non-compliance and suffering damage to our reputation. At the same time, we must ensure users can access data as required for them to work effectively.

It is not anticipated that this policy can eliminate all malicious data theft. Rather, its primary objective is to increase user awareness and avoid accidental loss scenarios, so it outlines the requirements for data leakage prevention.

2. Scope

2.1 In Scope

This data security policy applies all customer data, personal data, or other company data defined as sensitive by the company's data classification policy. Therefore, it applies to every server, database and IT system that handles such data, including any device that is regularly used for email, web access or other work-related tasks. Every user who interacts with company IT services is also subject to this policy.

2.2 Out of Scope

Information that is classified as Public is not subject to this policy. Other data can be excluded from the policy by company management based on specific business needs, such as that protecting the data is too costly or too complex.

3. Policy

3.1 Principles

The company shall provide all employees and contracted third parties with access to the information they need to carry out their responsibilities in as effective and efficient manner as possible.

3.2 General

a. Each user shall be identified by a unique user ID so that individuals can be held accountable for their actions.

b. The use of shared identities is permitted only where they are suitable, such as training accounts or service accounts.

c. Records of user access may be used to provide evidence for security incident investigations.

d. Access shall be granted based on the principle of least privilege, which means that each program and user will be granted the fewest privileges necessary to complete their tasks.

3.3 Access Control Authorization

Access to company IT resources and services will be given through the provision of a unique user account and complex password. Accounts are provided by the IT department on the basis of records in the HR department.

Passwords are managed by the IT Service Desk. Password must include an uppercase letter, lowercase letter, number and a symbol.

Role-based access control (RBAC) will be used to secure access to all file-based resources in Active Directory domains.

3.4 Network Access

a. All employees and contractors shall be given network access in accordance with business access control procedures and the least-privilege principle.

b. All staff and contractors who have remote access to company networks shall be authenticated using the VPN authentication mechanism only.

c. Segregation of networks shall be implemented as recommended by company network security research. Network administrators shall group together information services, users and information systems as appropriate to achieve the required segregation.

d. Network routing controls shall be implemented to support the access control policy.

3.5 User Responsibilities

a. All users must keep their workplace clear of any sensitive or confidential information when they leave.

b. All users must keep their passwords confidential and not share them.

3.6 Application and Information Access

a. All company staff and contractors shall be granted access to the data and applications required for their job roles.

b. All company staff and contractors shall access sensitive data and systems only if there is a business need to do so and they have approval from higher management.

c. Sensitive systems shall be physically or logically isolated in order to restrict access to authorized personnel only.

3.7 Access to Confidential, Restricted information

a. Access to data classified as 'Confidential' or 'Restricted' shall be limited to authorized persons whose job responsibilities require it, as determined by the Data Security Policy or higher management.

b. The responsibility to implement access restrictions lies with the IT Security department.

4. Technical Guidelines

Access control methods to be used shall include:

- *Role-based access model*
- *Web authentication rights*

Access control applies to all networks, servers, workstations, laptops, mobile devices, web applications and websites, cloud storages, and services.

5. Reporting Requirements

a. High-priority incidents discovered by the IT Security department shall be immediately escalated; the IT manager should be contacted as soon as possible.

6. Ownership and Responsibilities

- ***Data owners** are employees who have primary responsibility for maintaining information that they own, such as an executive, department manager or team leader.*
- ***Information Security Administrator** is an employee designated by the IT management who provides administrative support for the implementation, oversight and coordination of security procedures and systems with respect to specific information resources.*

- ***Users*** *include everyone who has access to information resources, such as employees, trustees, contractors, consultants, trials, temporary employees and volunteers.*

- ***The Incident Response Team*** *shall be chaired by an executive and include employees from departments such as IT Infrastructure, IT Application Security, Legal, Financial Services and Human Resources.*

7. Enforcement

Any user found in violation of this policy is subject to disciplinary action, up to and including termination of employment. Any third-party partner or contractor found in violation may have their network connection terminated.

8. Definitions

This paragraph defines any technical terms used in this policy.

- ***Access control list (ACL)*** *— A list of access control entries (ACEs) or rules. Each ACE in an ACL identifies a trustee and specifies the access rights allowed, denied or audited for that trustee.*

- ***Database*** *— An organized collection of data, generally stored and accessed electronically from a computer system.*

- ***Encryption****—The process of encoding a message or other information so that only authorized parties can access it.*

- ***Firewall*** *— A way of isolating one network from another. Firewalls can be standalone systems or can be included in other devices, such as routers or servers.*

- ***Network segregation*** *— The separation of the network into logical or functional units called zones. For example, you might have a zone for sales, a zone for technical support and another zone for research, each of which has different technical needs.*

- ***Role-based access control (RBAC)*** *— A policy-neutral access-control mechanism defined around roles and privileges.*

- ***Server*** *— A computer program or a device that provides functionality for other programs or devices, called clients.*

- ***Virtual private network (VPN)*** *— A secure private network connection across a public network.*

- ***VLAN (virtual LAN)*** *— A logical grouping of devices in the same broadcast domain.*