# ISMS Policy

| | | | |
|---|---|---|---|
| **Organization:** | Prime Numbers | **Document No:** | ISMS-01 |
| **Department:** | Security | **Revision:** | **1.0** |
| **Section:** | ISMS policy | **Sheet:** | **1 of 12** |

## Table of Contents

# ISMS Policy

## Document Control

### Document Version History

This table shows a record of significant changes to the document.

| Version | Date | Author | Description of Change |
|---|---|---|---|
| 1.0 | 12/07/2023 | Alejandro de la Cruz | Initial release |
| | | | |
| | | | |

**REVIEWERS**

| Name | Position | Date |
|---|---|---|
| | | |
| | | |
| | | |

**APPROVALS**

This table shows the approvals on this document for circulation, use, and withdrawal.

| Version | Date | Approver | Title/Authority | Approval Remarks |
|---|---|---|---|---|
| 1.0 | 20/01/2024 | Sitao Zhang | CTO | |
| 1.1 | | | | |
| 1.2 | | | | |

DISTRIBUTION

# ISMS Policy

| Version | Date | Distributed to | Distribution format |
|---|---|---|---|
| | | | |
| | | | |
| | | | |

# 1. Context of the organization

Rubyx utilizes advanced digital lending techniques to offer services like credit scoring, loan portfolio management, collection, and reporting, operating across multiple countries and offering crucial support to financial institutions and digital platforms that provide financial services.

Given the nature of our operations, Rubyx collects, processes, and stores a wide range of information pertaining to our customers, platform users, and individual and non-individual borrowers. The company uses data from client transactions to assess the financial health and repayment ability of potential borrowers.

Rubyx lending as a service platform does not require Personal Identifiable Information (PII). Rubyx only collects privacy data or PIIs with explicit customer consent, and we ensure the confidentiality of our information through non-disclosure agreements.

It is of utmost importance that all this information remains secure and confidential. The Information Security Policy is responsible for guaranteeing the confidentiality, integrity, and availability of all information and associated assets, safeguarding them against both external and internal threats, whether accidental or intentional.

As with internal and external issues stakeholders and their requirements and expectations were identified, Rubyx also identified the needs and expectations of interested parties and identified the opportunities and threats and the degree of risk attached to each.

# 2. Objectives

The Organization will retain documented information on the information security objectives. The objectives of the ISMS policy include the following:

- Confidentiality: Protect sensitive information from unauthorized access, disclosure, or theft.

- Integrity: Ensure that information is accurate, reliable, and not tampered with or modified inappropriately.

- Availability: Ensure that information is accessible to authorized users when needed and not lost or destroyed due to system failures or other events.

- Compliance: Ensure that the Organization complies with relevant laws, regulations, and standards related to information security.

- Risk Management: Identify and manage risks related to the Organization's information assets and take appropriate steps to mitigate those risks.

- Continual Improvement: Continuously monitor and improve the Organization's information security posture, including its policies, procedures, and technical controls.

# 3. Commitment

Rubyx Executive Leadership is fully committed to the establishment, implementation, operation, monitoring, review, maintenance, and improvement of the ISMS. Sufficient resources are dedicated to enable an efficient and proactive IS program. The ISMS Steering Committee ensures that all stakeholders remain informed. Additionally, the MRB confirms and monitors proactive coordination of activities between departments with overlapping responsibilities for information security including but not limited to Customer Success, Technology, and Data teams.

The committee reviews and approves all information security policies and procedures, as well as the management system for overall ISMS performance. The committee meets quarterly or on an ad hoc basis to review progress related to:

- Incident Management.
- Risk Assessment & Mitigation.
- Compliance with Regulations/Legislation.

# 4. Scope

Rubyx, a fintech company providing Lending-as-a-Service (LaaS) solutions to financial institutions and digital platforms, implements an Information Security Management System (ISMS) in accordance with ISO 27001.

**This ISMS covers production resources that directly support the Rubyx LaaS platform, including:**

1. **Data:** Customer, financial, and platform data processed by the LaaS platform, including loan information, credit scores, transaction details, and partner data.

2. **Systems and Applications:** The LaaS platform APIs, partner integrations, and any internal systems supporting LaaS operations.
3. **Processes:** Development, deployment, maintenance, and support of the LaaS platform, along with data exchange with partners and security incident response procedures.
4. **People:** Employees, contractors, and authorized users of LaaS platform clients with access to sensitive information.

**The scope of shared responsibility considerations includes**

Assets maintained and stored in the cloud computing environment, infrastructure assets management, processes that run on a multi-tenant virtualized environment, and cloud service administration.

**Excluded from the scope of ISMS:**

As an all-remote company, there are no physical office locations in the scope of the ISMS.

# 5. Responsibilities

Our leadership is fully committed to the Information Security Management System (ISMS) and recognizes its critical importance to our business operations and client trust.

Our ISMS policy is designed to protect our information assets, ensure business continuity, and reduce business damage by preventing and minimizing the impact of security incidents. It aligns with our strategic business objectives and compliance requirements.

Rubyx commits necessary resources including skilled personnel, advanced technology, and sufficient budget to maintain and improve the ISMS.

We are committed to the continuous improvement of the ISMS through regular reviews, audits, and updates in response to the evolving security landscape.

The leadership regularly reviews the ISMS performance through quarterly meetings and reports. Effectiveness is monitored using key performance indicators and internal audits.

The leadership regularly reviews the ISMS performance through quarterly meetings and reports. Effectiveness is monitored using key performance indicators and internal audits.

The leadership regularly reviews the ISMS performance through meetings and reports every 3 months. Effectiveness is monitored using key performance indicators and internal audits.

# 6. ISMS Policy

The Policy's goal is to safeguard Rubyx's information assets from any risks, whether internal or external, intentional or unintentional.

The Organization's Policy is to ensure that:

- As the business process requires, information should be made available with minimal disturbance to staff and the general public.
- The confidentiality of this data will be protected. Information confidentiality will be ensured, including but not limited to research, third parties, and personal and electronic communications data.
- All legal and regulatory standards will be met.
- Employees should get information security education, awareness, and training.
- All actual or suspected information security breaches must be reported to and investigated by the appropriate authorities, including System Administration and Incident Response.
- Appropriate access control will be maintained, and data will be kept safe from unwanted access. To complement the ISMS Policy, policies, procedures, and guidelines for Rubyx will be available through an intranet system in print and online forms.

## 6.1 Information Security Requirements

With the internal business and cloud service clients, a precise definition of information security requirements will be agreed upon and maintained. All ISMS work will be focused on meeting those criteria. Legislative, regulatory, and contractual agreements will also be documented and included in the planning process. As part of each project's design, specific security needs for new or altered systems or services will be captured.

The Rubyx ISMS's key idea is that controls are implemented in response to business needs, which will be conveyed to all employees via team meetings and briefing documents.

## 6.2 Risk Management

The ISMS policy defines risk management as a core component of the organization's approach to information security. It outlines the objectives and principles guiding the risk management process, as well as the roles and responsibilities of individuals involved. It involves understanding potential threats, vulnerabilities, and the potential impact of incidents on the confidentiality, integrity, and availability of information. The organization establishes a framework that promotes a proactive and systematic approach to identifying, assessing, and managing risks to their information assets.

## 6.3 Change Management

The ISMS policy defines change management as a critical component of the organization's overall information security strategy and provides guidance on how changes should be managed to minimize risks to information assets. It involves assessing the potential impact of changes on information security, implementing appropriate controls, and ensuring that changes are effectively planned, tested, and documented.

## 6.4 Human Resources

Based on proper education, training, abilities, and experience, Rubyx will ensure that all personnel involved in information security are competent. The required skills will be determined and assessed regularly, as well as an assessment of current skill levels within Rubyx. This Training will be done by all Rubyx employees in order to ensure a level of information awareness. The HR department will keep track of training, education, and other necessary data to document individual skill levels.

## 6.5 Business Continuity

Business continuity, within the context of an Information Security Management System (ISMS) policy, refers to the strategies, plans, and procedures put in place to ensure the organization can continue its critical operations and minimize the impact of disruptions or incidents that may threaten the availability of its information assets. It involves proactive measures to identify potential risks, develop resilience capabilities, and establish effective response and recovery mechanisms.

Rubyx defines business continuity as a fundamental aspect of the organization's information security strategy, highlighting the commitment to maintaining the continuity of business operations, safeguarding critical assets, and minimizing the impact of incidents.

## 6.6 Improvement of ISMS

Rubyx policy about continual improvement is to:

- Increase the level of proactivity (and stakeholder perception of proactivity) about information security, according to the Rubyx Policy on continuous improvement.

- Make information security processes and controls more measurable so that informed decisions may be made

- Evaluate important metrics yearly to see if they should be changed based on historical data.
- Collect ideas for continuous improvement through regular meetings and communication with stakeholders.
- In evaluating improvement recommendations, the following criteria must be used:
    - Cost
    - Business Benefit
    - Risk
    - Timeline for Implementation
    - Resources required

# 7. Policies and Procedures

Here is the list of policies and procedures that support ISMS:

| Policy | Purpose |
|---|---|
| Acceptable use policy | Establish guidelines and expectations regarding the appropriate and responsible use of an organization's information technology resources, systems, and networks. |
| Access Control Policy | Outline the rules and principles governing the granting, management, and revocation of access privileges to individuals within the organization. |
| Asset Management | Establish guidelines, procedures, and controls for effectively managing and protecting the organization's information assets throughout their lifecycle |
| Information classification policy | Establish a framework and guidelines for categorizing and labeling information assets based on their level of sensitivity, importance, and criticality to the organization. |
| Mobile Device and Teleworking Policy | Establish guidelines, procedures, and controls that ensure the security and protection of information assets when using mobile devices and engaging in teleworking or remote work arrangements. |

# ISMS Policy

| Policy | Purpose |
|---|---|
| Disposal and destruction policy | Establish guidelines, procedures, and controls for the secure and proper disposal of information assets that are no longer needed or have reached the end of their lifecycle. |
| Password policy | Establish guidelines, requirements, and best practices for the creation, use, and management of passwords within an organization's information systems. |
| Data recovery and backup policy | Establish guidelines, procedures, and controls for the regular and secure backup of critical information assets and the recovery of data in the event of a disruption, system failure, or data loss. |
| Cloud computing policy | Establish guidelines, controls, and best practices for the secure and effective use of cloud computing services within an organization and ensure the confidentiality, integrity, and availability of data and systems that are hosted or processed in the cloud. |
| Document and Record Control Procedure | Establish a systematic approach for managing and controlling the creation, distribution, access, storage, retention, and disposal of documents and records within an organization's information security management framework. |
| Cryptographic Standard | Provide guidelines, procedures, and controls for the proper and secure use of cryptographic techniques and technologies within an organization |
| BYOD Policy | Establish guidelines, procedures, and controls for the secure and responsible use of personal devices, such as smartphones, laptops, or tablets, that are owned by employees but used for work purposes within the organization. |
| Corrective Action Procedure | Establish a structured and systematic approach for identifying, addressing, and resolving non-conformities, incidents, and other issues related to information security within an organization |
| Disaster and Recovery Plan | Establish a structured and coordinated approach to mitigate the impact of disasters and facilitate the recovery of critical information systems and assets. |
| Information Security Guidance | Outlines the organization's commitment to information security and provides guidance for the development, implementation, and maintenance of the ISMS |

| Policy | Purpose |
|---|---|
| Information Transfer Policy | Establish guidelines, procedures, and controls for the secure and controlled transfer of information assets within and outside the organization. |
| Monitoring and Logging Policy | Establish guidelines, procedures, and controls for the monitoring, collection, and retention of system logs and security events within an organization. |
| Monitoring and Measuring Policy | Outlines the methods, frequency, and objectives of monitoring and measuring activities to ensure that information security controls are operating effectively and meeting the desired outcomes. |
| Network Security Design | Establish a secure and robust network infrastructure that protects the confidentiality, integrity, and availability of information assets within an organization |
| Patch and Vulnerability Management Policy | Establish guidelines, procedures, and controls for the timely and effective management of software patches and system updates within an organization's IT infrastructure. |
| Secure Development Policy | Establish guidelines, principles, and controls for ensuring the secure development of software and applications within an organization. The policy focuses on integrating security considerations throughout the entire software development lifecycle, from design to deployment. |
| Secure System Architecture and Engineering Principles | Provide guidelines, principles, and best practices for designing, implementing, and maintaining secure and resilient information systems within an organization |

# 8. Exceptions

- Only the CTO or his/her designated Officer may grant exceptions to the policies outlined in this document. Specific procedures for handling requests and authorizations for exceptions may be implemented in some circumstances.

- Every time a policy exception is triggered, a security log must be entered with the date and time, a description of the exception, the reason for the exception, and how the risk was managed.

- All IT services shall be used following the technical and security criteria established during service design.

- Policy violations may result in disciplinary action. They may even result in prosecution in some severe circumstances.

# 9. Performance Evaluation

Annual policy audits and reviews will be done, with any required adjustments made. In addition, security systems will be subjected to an independent examination.

Here are some methods used to measure the effectiveness of the ISMS

- **Key Performance Indicators (KPIs)**
  - **Policy compliance**: The percentage of employees who have read and acknowledged the ISMS Policy.
  - **Policy review frequency**: Number of times the Policy is reviewed and updated
  - **Policy exceptions**: The number of exceptions to the ISMS Policy granted.
  - **Policy completeness**: The extent to which the ISMS Policy covers all relevant areas of the Organization's information security.
  - **Policy effectiveness**: The degree to which the ISMS Policy effectively achieves its intended goals. The measure includes tracking security incidents, vulnerabilities, and other security metrics to determine if the Policy reduces the Organization's overall risk exposure.

- **Internal Audits**: The auditor should review the ISMS to ensure that it complies with relevant standards, policies, and procedures. The auditor should also identify any gaps or areas for improvement. During an internal audit of an ISMS policy, the auditor will review the Policy to ensure that it is up-to-date, accurate, and relevant. The auditor will also evaluate the implementation of the Policy to determine if it is being followed correctly and if any improvements can be made.

The internal audit process typically involves the following steps:

  - **Planning and preparation**: The auditor will identify the audit scope, determine the audit objectives, and develop an audit plan.
  - **Fieldwork**: The auditor will conduct interviews with key stakeholders, review documentation and records, and assess the effectiveness of controls.
  - **Reporting**: The auditor will prepare a report of their findings and recommendations for improvement.
  - **Follow-up**: The Organization will review and respond to the audit report and implement necessary corrective actions.

- **Management Reviews**: Regular management reviews will help ensure that the ISMS is aligned with the Organization's objectives and is operating effectively. The management team should review the performance of the ISMS and identify any areas for improvement. The review should include an analysis of the KPIs and the results of the internal audits. The management team should then develop an action plan to address any issues identified during the review.

# 10. Policy Review

The Organization implements the following steps in reviewing ISMS Policy:

- **Establish the review schedule**: The Organization determines the frequency of the policy review process. It is recommended to review policies annually or whenever there is a significant change in the Organization's environment.
- **Identify the policies to be reviewed**: The policies that require review and updating will be identified. This may include policies related to access control, data classification, incident management, and others.
- **Review the Policy**: The Policy will be reviewed to ensure that it is accurate, complete, and current. In addition, the review should consider any changes in the Organization's objectives, risk management strategy, or regulatory requirements.
- **Update the Policy**: The Policy will be updated to reflect any necessary changes. The revised policies are then communicated to all relevant stakeholders.
- **Approve the policies**: The revised policies should be approved by the appropriate personnel, such as senior management or the information security steering committee.
- **Implement the Policy**: After the policies have been approved, they should be implemented and communicated to all relevant stakeholders. This involves training or awareness programs to ensure employees understand and comply with the policies.
- **Monitor the policies**: Periodic audits or assessments will be conducted to evaluate the effectiveness of the Policy.

# 11. Confidentiality

All rights are reserved in this document, which is copyrighted. Without the previous written consent of an authorized representative of Rubyx, this document may not be copied, photocopied, reproduced, translated, or reduced to any electronic medium or machine-readable form, in whole or in part. This document is for internal use only and may be given to anybody outside the firm, including customers, clients, or prospects, after receiving consent from an authorized representative of Rubyx in whole or in part.