Information Security Management Systems Policy Document

ISO27001:2013 ISMS POLICY DOCUMENT

Version 1.2 – February 2017

Contents

1 INTRODUCTION

This document is the ISMS Policy Document of RippleRock Ltd. It is the property of RippleRock Ltd. and is a controlled document.

The purpose of the ISMS Policy Document is to provide an overview of the company, the activities it carries out and the quality standards of operation it conforms to. It is not designed to act as a procedure manual, although it does carry information about where procedures information is located and the detailed information on Documentation Requirements for essential procedures e.g. document control, and control of records; internal audit and corrective/preventative action (please see Procedures Log).

2 ISSUE STATUS

The issue status is indicated by the version number in the footer of this document. It identifies the issue status of this ISMS Policy Document.

When any part of this ISMS Policy Document is amended, a record is made in the Amendment Log shown below.

The ISMS Policy Document can be fully revised and re-issued at the discretion of the Management Team.

The ISMS Policy Document will be reviewed on a Quarterly basis as standard.

Please note that this ISMS Policy Document is only valid on day of printing.

Issue	Amendment	Date	Initials	Authorised
1	1st Authorised issue	Xxx	BA	BA

3 OVERVIEW OF RIPPLEROCK LTD

RippleRock Ltd provides consulting, training and coaching to companies adopting Agile ways of working. We have a global client base of over 40 companies.

We have developed a data visualisation tool that works on Team Foundation Services (Microsoft) and JIRA (Atlassian). We provide on-premise and cloud hosted versions of the application.

As a consequence of our business activity it is essential that we operate a clearly defined and robust approach to the security of our own and clients' data.

3.1 Scope of Registration

Provide cloud-based application to provide users with access to visual reporting on data held in the cloud versions of JIRA and Visual Studio Team Services (VSTS)

4 INFORMATION SECURITY MANAGEMENT SYSTEM

RippleRock Ltd. has a commitment to quality and a formal information security management system (ISMS) that addresses the following areas:

- Quality
- Performance monitoring and review
- Policy and Procedures
- Managing external relationships
- Financial Management
- Strategic and business planning
- Human resource development
- Service innovation.

4.1 DOCUMENTED INFORMATION

4.1.1 Documents

Policy and procedure documents are reviewed annually. Any documents requiring amendment are updated, authorised, and completed. All updates to documents are signed and dated by one of the Directors. Documents are re-issued as an electronic PDF document and a limited number of hard copies are produced.

Obsolete documents will be archived and restricted by the Director, electronic copies of all past versions are kept. All managers hold responsibility for cascading information to staff.

4.1.2 Records

All project records are stored in appropriate electronic folders and managed by respective departments.

Hard copies of documents are restricted to a minimum and should not be produced unnecessarily.

Electronic records are encouraged over hard copies due to environmental concerns, available storage space and to prevent unnecessary expenditure.

5. MANAGEMENT COMMITMENT

5.1 Role of Management

The RippleRock Ltd. Management Team are committed to the development and implementation of an Information Security Policy, an Information Security Management System, and to frequently review this system. Responsibility has been assigned to ensure that the ISMS conforms to the requirement of the standard and the provision to report on performance to the senior management team has been defined.

The Managing Director will ensure that RippleRock Ltd staff are aware of the importance of meeting customer as well as statutory and regulatory requirements, and overall, to contribute to achieving.

The RippleRock Ltd Information Security Objectives which are aligned with the current business plan.

The Management Team is responsible for implementing the ISMS and ensuring the system is understood and complied with at all levels of the organisation. They are responsible for ensuring that;

- The information security policy and objectives are established and in line with the strategic direction of the organisation
- Integration of the ISMS into the organisations processes.
- That resources needed for the ISMS are available
- Communication covering the importance of effective information security management and conformance to the ISMS requirements is in place.
- The ISMS achieves its intended outcome(s)
- The contribution of persons involved in the effectiveness of the ISMS by direction and support.
- Continual improvement is promoted
- Other management roles within their area of responsibility are supported.

An internal audit of procedures and policies is conducted annually in January. A review of the Information Security Objectives takes place in July.

6. ISMS POLICY

6.1 Introduction

This document is the Information Security Policy for RippleRock Ltd. It describes the company's corporate approach to Information Security and details how we address our responsibilities in relation to this vital area of our business. As a company we are committed to satisfy applicable requirements related to information security and the continual improvement of the ISMS.

Information Security is the responsibility of all members of staff, not just the management team, and as such all staff should retain an awareness of this policy and its contents and demonstrate a practical application of the key objectives where appropriate in their daily duties.

Verification of compliance with the policy will be verified by a continuous programme of internal audits.

6.2 Scope of the Policy

The scope of this policy relates to the application and databases that the company hosts in the Azure cloud. This application reads client data that is held within JIRA, as part of the Atlassian hosted solution or within Microsoft's cloud-hosted VSTS.

We maintain a number of flow charts which illustrate key business activities and their correspondence to ISMS requirements.

6.3 Legal and Regulatory Obligations

- Data Protection Act 1998
- Employment Agency Act 2003

6.4 Roles and Responsibilities

Our Information Security Manager is responsible for reviewing policies and access to data that we hold about clients. This data is not of sensitive nature, but relates to personalisation choices made by users and the details of charts they have saved in the application.

6.5 Strategic Approach and Principles

6.5.1 Information Classification

We hold a small range of data required to facilitate the application. This data is held within two databases, both of which are only accessible by RippleRock Ltd. Developers and management.

Access levels are relevant to the staff job role.

Security level	Definition	Examples
Confidential	Accessible to development team and management of the Ripple Rock Ltd.	Names and email addresses of license holders
Restricted	Accessible to development team and management of the Ripple Rock Ltd	Cached non-sensitive data from client projects
Protected	Accessible to development team and users of the application	Saved charts, queries to JIRA/VSTS instances, personalised settings e.g. favourite charts and saved chart details
Open	Accessible to all	Application help pages

6.5.2 Access Control

Users only have access to the projects from their organisation. Access to specific projects is controlled by their company and cannot be amended by RippleRock Ltd.

The application uses OAuth 2.0 JWT to authenticate users against their host application in JIRA/VSTS before they can access the SenseAdapt application and any saved charts. Users do

NOT have a separate password to access SenseAdapt – authentication is handled entirely by JIRA/VSTS.

Data segregation is enforced through a unique client identifier and is persistent through the application programming logic, the database table relationships, and the file system structure.

Access to the company business operations database and development environment is restricted by password. Passwords MUST NOT be written down either on paper or retained electronically. Passwords will be changed on a six monthly basis and the last twenty passwords may not be reused.

Passwords should be no less than 8 characters in length and consist of both numbers, cases and letters.

We use Azure user auditing and threat detection functionality in SQL server to track what the user has accessed within the application. We regularly review the audit logs.

6.5.3 Incident Management

Any and all incidents must be reported immediately in the first instance to the Managing Director or the Information Security Manager. Please refer to the Information Security Incident Document

6.5.4 Physical Security

All client data is held on remote servers located within Azure which has ISO27001:2005 level security in place.

Developers work from home offices. They do not hold client data locally. Screensavers lock the computers after 10 minutes when not in use. Every developer is expected to secure their machines.

Developers access the development environment over a secure 4096 bit encrypted connection.

6.5.5 Third-Party Access

We do not have any third party access to our systems.

6.6 Business Continuity Management

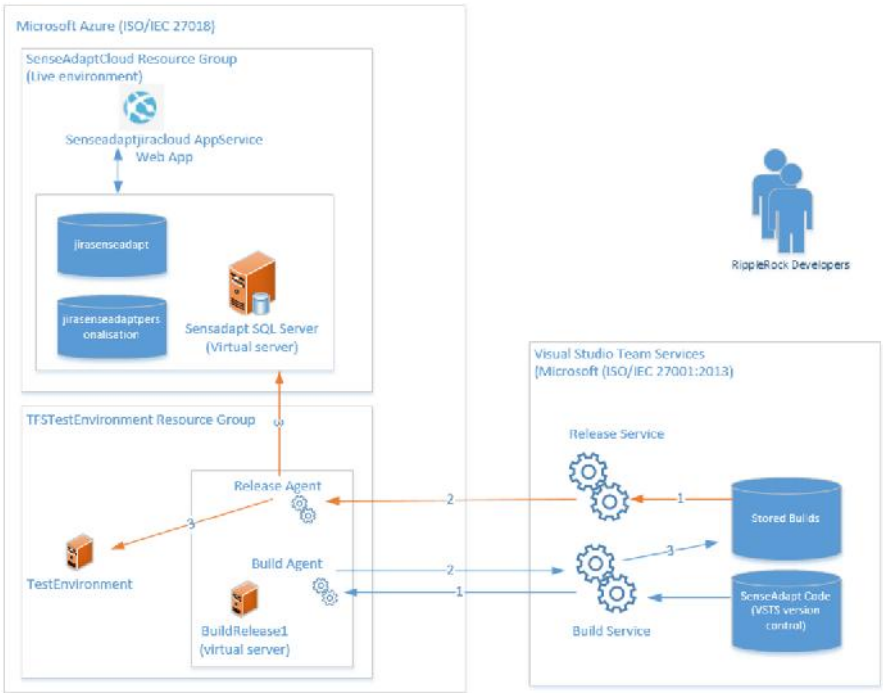
Our solution is hosted within Microsoft Azure an ISO/IEC 27018 accredited cloud services organisation. We have made extensive use of the features available within Azure and Microsoft VSTS (where our solutions code is hosted and it is deployed from) to help with business continuity management, these include.

Point-In-Time Database Backups

Our SQL Server databases in the Azure Environment makes use of Point-In-Time database restore, this functionality provides database point-in-time recovery up to 35 days from the current day.

Release Management Deployments

Our deployments are highly automated and configurable using Microsoft's VSTS Release Management service. In the event of the solutions website being compromised we can restore the website automatically to it previous states using MS Release Management. In the event a deployed build to the website fails, we can roll back our website to a previous working build within minutes.



6.7 Approach to Risk Management

We have carried out a full risk assessment of the potential for a breach of security as documented within our separate Risk Assessment Document.

We aim to reduce all opportunities for data to be compromised. This includes the possibility of theft of data.

6.7.1 Action in the event of a policy breach

Access to the system is centrally controlled and removal of access to the system is a simple procedure, controlled by the Information Security Manager.

Immediately a policy breach has been detected any relevant user is either removed or reset depending upon the most appropriate action in the circumstances.

6.8 Information Security Objectives

Our objectives are detailed in our Security assessment document. Each member of staff is aware of these objectives and they are reviewed and discussed at least once per year in our regular team offsites.

The objectives are as follows:

- **Objective 1: Existing services** – RippleRock Ltd. will continue to deliver its services within a secure environment
- **Objective 2: Development -** RippleRock Ltd. will conduct annual risk assessments to ensure that risk to information in the care of RippleRock Ltd. is minimised or eliminated.

6.9 Responsibility, Authority and Communication

As a small company of 8, RippleRock Ltd has a flat management structure. Everyone reports directly to one of the two Directors.

The Information Security Officer looks after the environments, access and process governance.

6.9.1 Management Representative

The Information Security Officer is responsible for the maintenance, measurement and review of our Information Security Management System. The Information Security Officer will ensure that the processes needed for the Information Security Management System are established.

In addition he/she will report to SMT about system performance.

6.9.2 Internal Communications

Internal communication is through email and Slack. An auditable record of both systems is maintained.

6.9.3 Implementation

Following the annual audit, results will be collated and disseminated through the internal communications framework:

6.10 Management Review

6.10.1 General

Senior Management ensures:

- That the ongoing activities of RippleRock Ltd are reviewed regularly and that any required corrective action is adequately implemented and reviewed to establish an effective preventative process
- Measurement of RippleRock Ltd performance against our declared Information Security Objectives
- That internal audits are conducted regularly to review progress and assist in the improvement of processes & procedures. The reviews will be discussed as part of RippleRock Ltd management meetings
- That employees have the necessary training, support, specifications and equipment to effectively carry out the work. The management team hold planning and review meetings every month. Minutes of these are taken and the agenda normally includes an update and discussion around the current work of all departments and services.

6.11 Review Input

The daily stand-up is used to review any changes to functionality, performance or security. Reviews of code and policies ensure good practise in the updating and backing up of databases.

6.11.1 Implementation

The development team meets for a daily stand-up at 9:30.

Weekly 'Ripple Sync' calls review the broader company situation

All actions are captured in TFS Agile boards and tracked through to completion. These auditable logs of work and responsibility can be used if a situation requires detailed review.

6.12 Review Output

The Management Team reviews produce the following outputs:

- Policies and procedures are updated to make operations more efficient
- Operations and services are improved through measurement against targets and actions to improve or rectify specific areas.
- Where resources are lacking actions are put in place to rectify this.

6.12.1 Implementation

- Corrective actions are identified and recorded in the Agile process board
- Progress is monitored in relation to other priorities
- Situation re-evaluated at a specified later date.

7 PROVISION OF RESOURCES

RippleRock Ltd will provide all the resources needed to implement and maintain the applications and support for clients. This will be reviewed through audits, user surveys and continuous improvement.

7.1 Human Resources General

7.1.1 Competence, Awareness & Training

We review training needs and use a combination of mentoring, pair programming and training courses to ensure that we have the requisite skills.

7.2 Infrastructure

The procurement and management of hardware, software and supporting services such as communication and information systems are coordinated by the Information Security Manager.

We maintain a detailed asset register, including serial numbers, description and location or person to whom assigned.

7.2.1 Implementation

Both hardware and software is reviewed on an ongoing bases to ensure that staff are equipped with IT equipment and software that is necessary to do the job and support our customers

8 RISK ASSESSMENT METHODOLOGY

We have identified the following process as a means of conducting regular risk assessments relating to Information Security Issues.

Within each of these areas the risks (if any) are identified together with a rating as to the importance of the risk. The associated consequence or severity of the risk is also rated together with the probable likelihood of the risk occurring.

We use an Excel spreadsheet to collect and analyse the risks identified in the following assets / asset groups:

- Hardware – desktops. Laptops, removable media
- Software applications
- Infrastructure / servers
- Client information and data
- People and reputation
- Key contacts
- Critical third party suppliers

All typical / likely threats have been assessed based on their potential effects on Confidentiality, Integrity and Availability (CIA attributes) using a ratings scale of;

Very Low - 1, Low – 2, Medium – 3, High 4 and Very high – 5 and expressed across key areas of

Vulnerability, Probability and Impact

Following this analysis evaluations are drawn as to what the most appropriate action is together with the estimated cost of implementing action to address the identified issue and an estimate of the cost of ignoring the risk.

Key evaluation criteria we use is 1 – Accept risk, 2 - Apply controls, 3 - Avoid risk, 4 – Transfer the risk.

8.1 Risk Treatment Plan - Statement of Applicability

Our risk treatment plan has been designed and implemented using the main headings within the standard (Annex A Table A.1 – Control objectives and controls) as a guide to establish that all controls required have been considered and that there are no omissions.

The document identifies controls to mitigate risks following the process of identification, analysis and evaluation described in section 7 and is directly linked to the aspects of the organisation.

This document is kept within a secure file titled ISO270001 within the document section of the SharePoint portal

9 MEASUREMENT, ANALYSIS & IMPROVEMENT

9.1 Information Security Standards

We continually monitor usage of our applications including performance and user satisfaction levels.

We have agreed targets to resolve any issues which are detailed in the JIRA / VSTS marketplace for the SenseAdapt product.

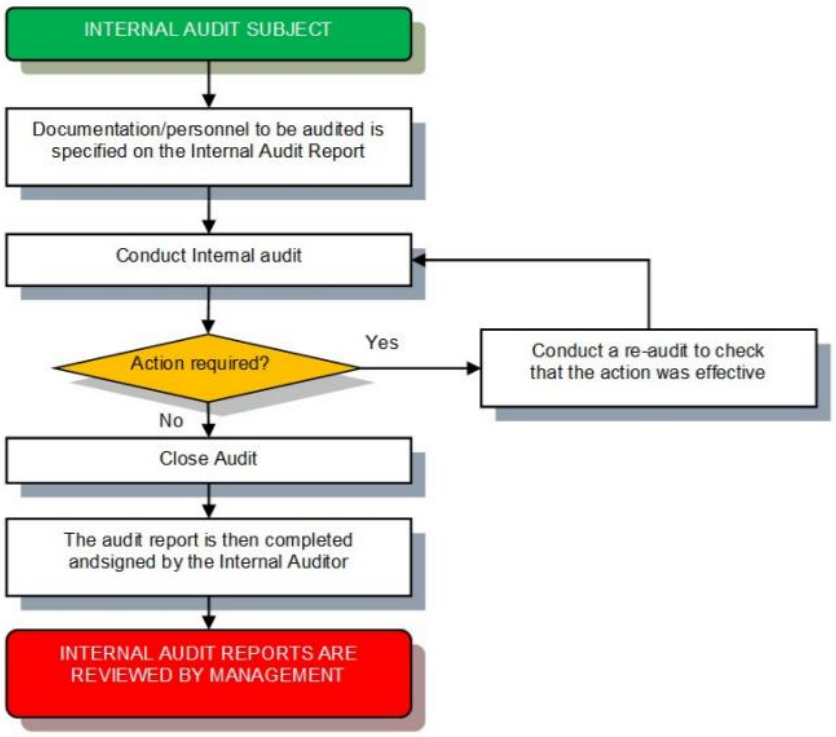
9.1.1 Implementation

We review the service provided on a daily basis. Support and bugs are tracked in Incident Tracking System and mitigating actions are held in TFS and managed through a Kanban process. We continually review cycle time and incident rates.

9.2 Internal ISMS Audits

The internal audit process is as follows:

9.2.1 Internal Audit Process Flowchart



Commented [RS1]: If we are going to use these diagrams I am a lot more comfortable if we redo them.

Commented [AG2R1]: C+P to paint, change the colours hehe

Commented [BA3R1]: Rory to redo in Visio – SenseAdapt colours

9.3 Monitoring & Measurement of Process

9.3.1 Implementation

We review process and look to improve through regular team retrospectives. Improvement actions are all entered into TFS, prioritised and tracked through to completion.

9.4 Monitoring & Measurement of Service

We continually monitor performance of the application. We use the Azure auditing and threat detection service to monitor the database.

We also conduct quarterly penetration tests of the application by an external Third Party.

Third party cloud-based performance monitoring services provide us with real-time analysis of the application.

9.5 Analysis of Data

Incidents are tracked through TFS and the Incident Tracking System. Code quality and infrastructure logs are reviewed by the development team.

A regular technical review is undertaken based on common themes and trends seen with areas of concern raised as priority work.

9.5.1 Implementation

Data is collected as part of the part of the ongoing management of the site. Logs are reviewed and reported on using standard tools and queries.

9.6 Continual Improvement

Regular team retrospectives and ways of working ensure that we continuously review the application, architecture, coding standards, automated testing and ways of working. Specific actions are recorded in TFS and tracked through to completion.

9.6.1 Implementation

Regular retrospectives identify issues, identify root causes and capture improvement actions which we prioritise and put into TFS.

9.7 Corrective Action and Improvement

Regular meetings will review compliance and take any corrective actions. These will be tracked and be auditable through TFS. We will also review the suitability, adequacy and effectiveness of our ISMS.

9.8 Complaints Policy

The application has a clear link to enable users to raise an issue or provide us with feedback on any aspect of the application. All issues are tracked in our Incident Tracking System and reviewed as part of the daily stand-up.

9.9 Preventative Action

We continuously update the application and can respond relatively quickly to issues. We continue to increase levels or automation to enable us to avoid introducing new issues and to rapidly fix any issues that have been raised with us.

The team tracks the latest security bulletins and takes appropriate action.