ICT Change Management Policy

1. Intro

The purpose of this policy is to outline how changes are implemented in the RiskPoint Group's IT systems by employees and vendors.

The RiskPoint Group's change management process for ICT-related systems, covers changes to software, hardware, firmware components, and system and security parameters. This policy applies to the RiskPoint Group on a global basis.

2. Internal Applications

The RiskPoint Group has three internal development teams, each having separate release schedules, and variations on workflow, but all adhere to the below overall principles of Change Management. All change management processes:

- Plan changes for implementation
- Test changes prior to implementation
- Document changes based on what is changed, why the change is implemented, who owns the change, and dates regarding the change
- Contain fallback mechanisms into a latest stable build
- Have ways of overruling normal procedures in case of an emergency

APP software

The RiskPoint Group's main developer team uses JIRA as a project management tool to facilitate planning, prioritization, and communication.

The process begins with creating and maintaining a comprehensive backlog in JIRA, which includes stories and sub-tasks. The stories of the backlog primarily originates from meetings or requests from the RiskPoint Group employees. The backlog serves as a repository for all potential work, allowing prioritization. Regular planning sessions are conducted where the team collaborates in selecting the most critical tasks from the backlog.

After a story is completed, the responsible team member writes a summary that highlights the key features, improvements, or bug fixes associated with that particular task. As these summaries are written, they are stored and categorized.

Certain changes will made into cases for a software tester to assess before the change is released to the production environment. If changes fail or create issues with a significant business impact, it will be reported to IT management.

Business Intelligence

The Business Intelligence (BI) Team uses Jira to support an agile development methodology. The BI development cycle is based on 10 day Sprints with predefined work capacity and prioritization of planned tasks. Daily stand-up meetings are conducted by the team and the Jira backlog is regularly reviewed with relevant business owners. Bug fixes and enhancements are subject to functional testing by end-users before being approved. All code is stored in GitHub and is peer-reviewed prior to promotion into production environments.

The M&A Management System (Stella)

Changes to the RiskPoint Group's internal M&A Management System are documented by the developer via a bespoke document which is continuously updated.

The developer in charge of the tool creates changes on an ad-hoc basis. Changes are tested separately for functionality, and are published during low-activity periods to insure error-finding does not affect business.

Old application versions are continuously backed up, and roll-backs can happen to the latest stable build if deemed necessary.

Whenever a change to existing security measures are made, this application follows the same internal measures as the main IT infrastructure. As such, considerations regarding the effect of the changes are built into the overall security measure assessment.

3. Hardware / Firmware / Systems or security parameters

Procurement of new hardware is initiated by the applicable department manager, who sends the request to IT Management for approval. If approved, IT Management forwards the request to IT support who orders and enrolls the new device in the RiskPoint Group asset management system with a predefined image. This process is documented via Jira.

In non-headquarter locations, individual country managers are mandated to order hardware. When the order is delivered, the primary user of that device will contact IT support to enroll it in the device management system.

For certain types of hardware (phones and laptops), IT support keeps a change log of who holds a specified device.

4. External Applications

The Riskpoint Group requires vendors of core applications to document changes and send, or otherwise make available, monthly release notes to the RiskPoint Group.

Changes made by vendors to the RiskPoint Group's hosting environment requires approval from the IT department before being implemented. If it is found relevant, major changes must include roll back plans that will be discussed during implementation planning. This is done for cases of unforeseen consequences occurring after the changes have taken effect.

For more information about vendor management, please refer *to* our vendor management policy.

This policy is reviewed and updated annually.

Version: 1

Dated: February 2, 2025