Security Incident Response Policy

This policy outlines the responsibilities undertaken by Rico Technologies Limited (we, us, our) and our Customers (you, your) to avoid, respond to and mitigate security incidents.

Our responsibilities

Security Monitoring and Detection: We endeavour to implement and develop robust security measures to monitor and detect security threats and incidents such as intrusion detection systems, firewalls, and other security tools.

Incident Response: When a security threat is detected, we will promptly investigate and assess the nature and scope of the threat.

Notification: If the security threat poses a risk to customer data or systems, we will notify the affected customer(s), including details on the incident and the steps being taken to mitigate it.

Mitigation: We will take immediate action to mitigate the security threat, prevent further damage, and restore services as quickly as possible.

Root Cause Analysis: After resolving the incident, we will conduct a root cause analysis to determine how the threat occurred and take steps to prevent similar incidents in the future.

Transparency: We will maintain transparency with the affected customers throughout the incident response process, providing updates on progress and any necessary actions required from the customer.

Your Responsibilities

Notification: The customer should promptly notify Rico if they suspect or detect any unusual activity or potential security threats related to their use of the SaaS platform. You can report these to support@rico.nz.

Collaboration: In the event of a security incident, the customer should cooperate with our incident response efforts, providing necessary information and access to facilitate the investigation and resolution of the incident.

Compliance: You should ensure that you are using Rico in compliance with our Terms and Conditions.