Rundata Systems

Incident Reporting Plan

1 Purpose

The purpose of this incident reporting plan is to establish a clear and efficient process for reporting and addressing security incidents at Rundata Systems. This plan ensures that incidents are promptly detected, reported, and effectively responded to, minimizing potential damages and facilitating timely resolution.

2 Incident Types

Security incidents that should be reported under this plan include, but are not limited to: - Unauthorized access or use of systems or data - Malware infections or suspected compromises - Data breaches or leaks - Denial of service attacks - Physical security breaches - Any other suspicious or unusual activities that may compromise the security or integrity of Rundata Systems' systems, data, or infrastructure

3 Reporting Procedure

In the event of a security incident, follow these steps to report it:

Step 1: Initial Detection and Assessment

- Immediately upon detecting a security incident or suspecting its occurrence, take appropriate actions to mitigate any ongoing threats or damages.
- Assess the severity and potential impact of the incident.

Step 2: Detailed Incident Report

- Prepare a detailed incident report that includes the following information:
  - Incident description and timeline
  - Affected systems, applications, or data
  - Evidence or indicators related to the incident
  - Actions taken to mitigate the incident
  - Initial assessment of impact and potential risks
  - Any additional relevant information

Step 3: Incident Response and Recovery

- Collaborate with relevant Stakeholders to address the incident promptly and effectively.
- Preserve any evidence or logs that may be necessary for further analysis or legal purposes.

4 Incident Response Team Contacts

The following individuals and contact information serve as the Incident Response Team for Rundata Systems:

- Lelanthran Manickum: Director
  - Email: lee@rundata.co.za
  - Phone: +27 65 254 1792

5 Communication and Documentation

- All incident reports, communication, and related documentation should be appropriately logged and stored for future reference and analysis.
- Ensure that incident reports and associated information are handled with confidentiality and only shared with authorized personnel.

6 Plan Review

- This incident reporting plan will be reviewed and updated periodically to address any changes in the business environment, technologies, or incident response requirements.
- Incident response drills and exercises may be conducted to test the effectiveness of the plan.