Security Incident Response Plan

Kicol Tecnologia e Serviços LTDA

Document:	Security Incident Response Plan
Version:	1.0
Approval date:	March 3, 2026
Next review:	March 2027
Approved by:	Eduardo Macedo — Director / Technical Lead
Classification:	Internal use

CNPJ: 64.973.433/0001-06

Rua Alcindo Guanabara, 17, Sala 1313, Centro, Rio de Janeiro - RJ, 20031-130

1. Purpose

To define the procedures for identifying, containing, eradicating, recovering from and communicating information security incidents at Kicol Tecnologia e Serviços LTDA, minimizing the impact on operations and client data.

2. Incident Classification

Severity	Description	Response time
Critical	Client data breach, unauthorized production access, ransomware	Immediate (up to 1 hour)
High	Exploited vulnerability, service outage, compromised credentials	Up to 4 hours
Medium	Blocked unauthorized access attempt, anomalous behavior	Up to 24 hours
Low	Informational alerts, blocked phishing attempts	Up to 72 hours

3. Response Stages

3.1 Identification

Continuous system monitoring through server logs, hosting provider alerts and application monitoring. Any anomalous behavior is treated as a potential incident.

3.2 Containment

- Immediate isolation of the compromised resource;
- Revocation of potentially compromised credentials;
- Blocking suspicious IPs or access;
- Preservation of logs and evidence for later analysis.

3.3 Eradication

- Root cause identification and removal;
- Correction of the exploited vulnerability;
- System and dependency updates if necessary;
- Verification that no other points are compromised.

3.4 Recovery

- System restoration from intact backups when necessary;
- Verification of restored data integrity;
- Gradual service reactivation with intensified monitoring;
- Generation of new credentials and keys when applicable.

3.5 Notification

For incidents involving client data, the client will be notified within 48 hours with a description of the incident, containment measures and recommendations. For incidents involving personal data, notification to Brazil's National Data Protection Authority (ANPD) will be made as required by the LGPD.

3.6 Lessons learned

After each incident, an analysis is conducted to identify causes, evaluate response effectiveness and define preventive actions. The incident record is maintained with date, description, impact, actions taken and improvements implemented.

4. Review

This plan will be reviewed annually or after any significant security incident.

Version	Date	Description	Owner
1.0	03/03/2026	Initial version	Eduardo Macedo

5. Approval

_____

Eduardo Macedo
Director / Technical Lead
Kicol Tecnologia e Serviços LTDA
March 3, 2026