RSECURE

MADE IN LUXEMBOURG

Rsecure

RFC-2350

Rsecure sàrl ◆ 38-40, Parc d'Activités L-8308 Capellen ◆ Luxembourg
Tél.: +352 26 60 26 06 ◆ www.rsecure.lu
RCS Luxembourg : B256460 ◆ Matricule : 20212445771 ◆ TVA: LU33277706

Table des matières

1. ABOUT THIS DOCUMENT 3

A) DATE OF LAST UPDATE 3
B) DISTRIBUTION LIST FOR NOTIFICATIONS 3
C) DOCUMENT LOCATION 3
D) AUTHENTICITY 3

2. CONTACT INFORMATION 4

E) TEAM NAME 4
F) PHYSICAL ADDRESS 4
G) TIME ZONE 4
H) TELEPHONE NUMBER 4
I) ELECTRONIC MAIL ADDRESS 4
J) PUBLIC KEYS AND ENCRYPTION 4
K) MANAGEMENT AND POINTS OF CONTACT 4
L) PGP KEYS AND FINGERPRINTS 4

3. CHARTER AND MANDATE 5

M) MISSION STATEMENT 5
N) CONSTITUENCY 5
O) AUTHORITY AND SPONSORSHIP 5

4. POLICIES AND GOVERNANCE 6

P) TYPES OF INCIDENTS HANDLED 6
Q) COOPERATION AND INFORMATION SHARING 6
R) COMMUNICATION AND ENCRYPTION 6

5. SERVICES OFFERED 7

S) REACTIVE SERVICES (INCIDENT MANAGEMENT) 7
T) PROACTIVE SERVICES (INCIDENT PREVENTION) 7

6. INCIDENT NOTIFICATION FORM 8

7. DISCLAIMER 9

1. About this Document

a) Date of Last Update

June 8, 2026.

b) Distribution List for Notifications

No public distribution list is maintained at this time.

c) Document Location

The definitive version of this document is available on the official website at rsecure.lu.

d) Authenticity

This document is digitally signed using the Rsecure CSIRT public PGP key (see Section 2).

2. Contact Information

e) Team Name

R-CSIRT

f) Physical Address

Rsecure Sàrl, 38-40, Parc d'activités, L-8308 Capellen, Grand-Duché de Luxembourg.

g) Time Zone

Europe/Luxembourg (GMT+1 / GMT+2 during Daylight Saving Time).

h) Telephone Number

+352 20 60 26 06.

i) Electronic Mail Address

General contact: contact (a) rsecure.lu.

Incident reporting: csirt (a) rsecure.lu

j) Public Keys and Encryption

For reporting security incidents, the use of PGP-encrypted email is highly recommended.

k) Management and Points of Contact

The team operates under the direct leadership of Luc Cottin, CEO of Rsecure.

l) PGP Keys and Fingerprints

ID: AB57 4940 8331 D4EC
Fingerprint: 48EFDF6FB8521D14EFDEB21CAB5749408331D4EC

3. Charter and Mandate

m) Mission Statement

The mission of the R-CSIRT is to protect the IT infrastructures of private sector enterprises, particularly SMEs and entities operating within regulated industries (DORA, NIS2, ISO 27001) in Luxembourg. The team acts to minimize the impact of cyberattacks and assist in remediation efforts.

n) Constituency

Contracted clients under the Cybermonitoring / SOC managed services framework, Rcarre and Rcube's internal networks and customers.

o) Authority and Sponsorship

Rsecure operates as a private Luxembourgish service provider and is subsidiary of Rcarre.

4. Policies and Governance

p) Types of Incidents Handled

The CSIRT manages all types of computer security incidents, including server compromises, ransomware attacks, data exfiltration, and credential leaks.

q) Cooperation and Information Sharing

Rsecure strictly complies with GDPR requirements and Luxembourgish professional secrecy laws.

Rsecure will cooperate with all Rcarre entities.

r) Communication and Encryption

The preferred method of contact is email. All sensitive data, technical evidence, or incident reports exchanged via email must be encrypted using PGP or other means.

5. Services Offered

s) Reactive Services (Incident Management)

- Triage: Alert validation, severity categorization, and potential business impact assessment.
- Coordination: Technical liaison between the client's internal teams, third-party software vendors, and, if required, Luxembourgish regulatory bodies.
- Resolution & Forensic Analysis: Technical log review, threat containment, eradication of unauthorized access, and recovery assistance.

t) Proactive Services (Incident Prevention)

- Continuous monitoring (SOC) of corporate infrastructures to detect early signs of malicious activity.
- Pen test : detection of vulnerabilities on existing environments
- Audits of cybersecurity posture
- GRC: Risk assessments and compliance alignment with ISO 27001, DORA, and NIS2 regulations.
- CISO as a service
- Awareness Training & Testing: Security awareness programs aimed at reducing human cyber risk.

6. Incident Notification Form

To report a security incident, the notifying party should provide the following details to csirt@rsecure.lu:

- Full contact details of the reporter (Name, organization, phone number).
- Description of the anomaly (Suspicious behavior, ransom demand, suspected data leak).
- Affected systems and assets (IP ranges, critical servers, workstations, cloud services).
- Precise timestamp of the first detected events.
- Secure attachments (Log extracts, malicious email headers, screenshots).

7. Disclaimer

While Rsecure applies its full professional expertise to contain, analyze, and resolve information security incidents, it cannot be held liable for any indirect damages, operational downtime, or data loss resulting from a cyberattack suffered by its clients or third parties.