# 1. DOCUMENT INFORMATION

This document provides a description of Kindred Group CSIRT, based on the RFC2350.

## 1.1. Date of Last Update

Version 1.1, last updated on the 2021-01-22.

## 1.2. Distribution List for Notifications

There is no distribution list for notification.

## 1.3. Locations where this Document May Be Found

The latest version of this document can be found on the Kindred Group website contact page: https://www.kindredgroup.com/contact/

# 2. CONTACT INFORMATION

## 2.1. Name of the Team

Kindred Group CSIRT

## 2.2. Address

Kindred Group Security - CSIRT

Regeringsgatan 29

Floor 9

111 53 Stockholm

## 2.3. Time Zone

Europe/Stockholm

## 2.4. Telephone Number

+46 84 622 300

## 2.5. Facsimile Number

None

## 2.6. Electronic Mail Address

csirt@kindredgroup.com

## 2.7. Other Telecommunication

None

## 2.8. Public Keys and Encryption Information

Sensitive information can be sent encrypted using the GPG key below which is available on the same Contact page as this document.

| | |
|---|---|
| User ID: | csirt <csirt@kindredgroup.com> |
| Fingerprint: | D072 0E57 048C 2F65 778A 22DB E0AD 9ECE 34E0 1E44 |
| Key type: | RSA/4096 |
| Expires: | 2024-07-09 |

The key can be downloaded from keys.openpgp.org:
https://keys.openpgp.org/search?q=csirt@kindredgroup.com

## 2.9. Team Members

Kindred Group CSIRT team members are security analysts who work in the Kindred Group Security Team.

## 2.10. Other Information

None

## 2.11. Points of Customer Contact

The preferred method of contact is by email or, if urgent, by phone during Business Hours.

The CSIRT's business hours are 0900-1700, Stockholm time, Monday to Friday.

A 24/7 phone number contact can be provided to partners who would wish to report us urgent cases outside of business hours.

# 3. CHARTER

## 3.1. Mission Statement

Kindred Group CSIRT missions are to:

- Centrally coordinate security incidents happening within the constituency
- Perform security incident response tasks as well as forensics investigations
- Deliver post-mortem analysis of incidents, as part of a continuous improvement strategy
- Relay external security advisories to the internal teams
- Perform security awareness campaigns towards internal users
- Centrally coordinate the vulnerability management efforts
- Provide internal teams with hardening guidelines

## 3.2. Constituency

Kindred Group CSIRT's constituency is composed of all assets of Kindred Group IT and network systems, including but not limited to its users, networks, applications and systems.

## 3.3. Affiliation

Kindred Group CSIRT is affiliated to Kindred Group plc.

## 3.4. Authority

Kindred Group CSIRT operates under the authority of the Group Head of Security.

# 4. POLICIES

## 4.1. Types of Incidents and Level of Support

Kindred Group CSIRT centrally manages all security incidents reports occurring within the constituency.

The team triages the reports and assigns a severity ranking to incoming reports.

The level of support provided depends on the internal severity ranking, the actions required (incident response, coordination, digital forensics, ...) as well as the staff availability.

## 4.2. Co-operation, Interaction and Disclosure of Information

Kindred Group CSIRT acknowledges the importance of cooperation and exchange of information in the security field, within or outside its industry. Any similar organization (CERT, CSIRT, SOC, ...) can contact us to setup information sharing channels when there is a mutual benefit for the source and destination organization.

## 4.3. Communication and Authentication

Kindred Group CSIRT uses the FIRST TLP (Traffic Light Protocol) version 1.0 for communications received and sent to external parties.

The four TLP levels are mapped to our internal document sensitivity levels to make sure external sensitive information is not declassified once it reaches our organization.

Communication security (authentication and encryption) is achieved using GPG (preferred) or any other secure communication protocol agreed on with the different stakeholders.

# 5. SERVICES

## 5.1. Incident Response

Kindred Group CSIRT provides Incident Response services for incidents happening within or impacting its constituency.

### 5.1.1. Triage

Kindred Group CSIRT acts as a central point of escalation for Security Incidents. The Security Incident Reports are received by the team, triaged, categorized and, depending on the severity, either taken care of directly or escalated internally to be coordinated.

### 5.1.2. Coordination

Kindred Group CSIRT acts as a coordination body for Security Incidents, bringing together teams from different departments to contain and investigate incidents in a timely manner as well as keeping other important stakeholders informed of the ongoing events and their impact.

### 5.1.3. Investigation and Forensics

Kindred Group CSIRT provides Security Investigation as well as forensics services for our consistuency.

## 5.2. Proactive Activities

### 5.2.1 Alerts and Warnings

Kindred Group CSIRT provides information on security alerts, threats or vulnerabilities to the different stakeholders within the consistuency as well as advices on how to protect them.

### 5.2.2 Intrusion Detection Services

Kindred Group CSIRT and its SOC team provides the consistuency with Intrusion Detection Capabilities.

### 5.2.3 Awareness building

Kindred Group CSIRT creates and manages internal security awareness campaigns to build a security culture within the consistuency.

## 6. INCIDENT REPORTING FORMS

There is no externally pre-made form. Email contact using the address csirt@kindredgroup.com is preferred.

If the report contains sensitive information or PII, please send us an email on csirt@kindredgroup.com using our team GPG key for encryption.

If you want to report a vulnerability on one of our plateforms, please submit it through our Bug Bounty program: https://hackerone.com/kindred_group.

## 7. DISCLAIMERS

While every precaution will be taken in the preparation of information, notifications and alerts, Kindred Group CSIRT assumes no responsibilityfor errors or omissions, or for damages resultingfrom the use of the information it provides

## 8. DOCUMENT HISTORY

- Version 1.0: Initial document
- Version 1.1: Adding external link to keys.openpgp.org for the GPG key.