

Security Incident Response (CSIRT)

Purpose

This document describes the process for handling security incidents that affect ICT infrastructure systems.

For the German original, see here: [Security Incident Response \(CSIRT\)- Sicherheitsvorfall - ICT Infrastruktur](#)

- [Purpose](#)
- [General Infos](#)
- [Security Incident Procedure](#)
- [CSIRT Partner Contacts](#)

General Infos

The document describes the process for handling security incidents that affect ICT infrastructure systems. However, it only briefly outlines the approach to be taken in the event of a large-scale attack that may have already contaminated the systems (e.g., ransomware). In such cases, the BCP (Emergency Incident) is applied.

The following events are considered security incidents:

- Reporting of a security vulnerability by known sources (internal, Melani, CDC, CVE, etc.)
- Reporting of a security vulnerability by software vendors (Microsoft, EDR, OpenSource, etc.)
- Discovery of a weakness due to inadequate or missing configuration
- Awareness of an increased threat level due to cyber attacks

This list of events is not exhaustive.

In general terms, this process applies to all incidents that threaten the smooth operation of ICT infrastructure and associated business structures.

The Computer Security Incident Response Team (CSIRT) is responsible for handling security incidents. The team consists of the following members:

Administrative (at least 1 Person)

- Markus Berner, CIO

- Erich Stüssi, Head of ICT Infrastructure (Lead)
- Florian Ruf, Service Desk Leader
- Matthias Anderau, ICT Project Manager

Technical (at least 1 person from Server Solutions & 1 Person Network Solutions)

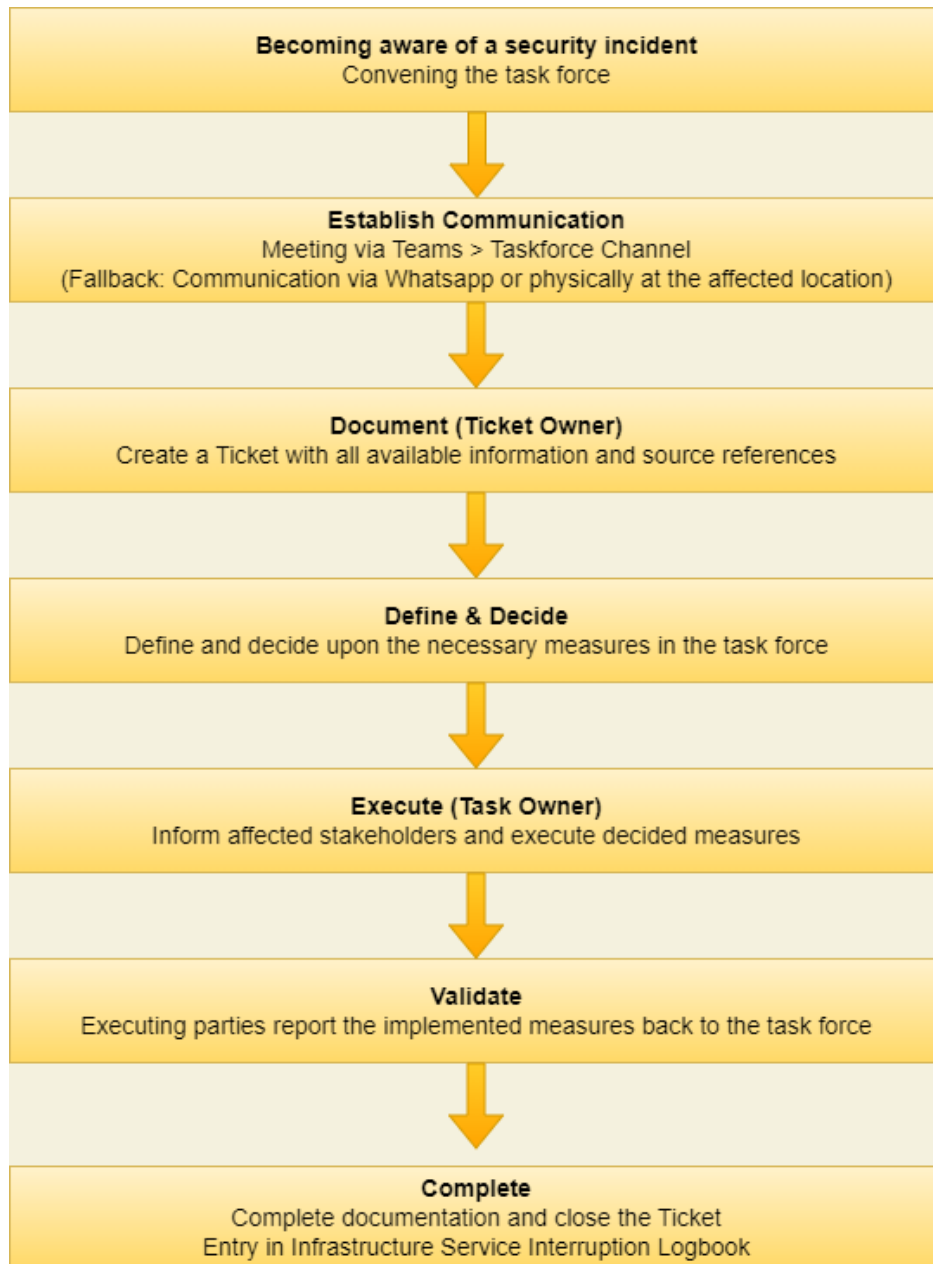
- Dominik Müller, ICT Solutions Server Leader
- Ueli Rütli, ICT Solutions Network Leader
- Samuel Frei, System Engineer (SCCM)
- Tony Fichtner, Service Desk Coordinator

Security Incident Procedure

When a security incident is detected, the Security Taskforce will be convened and a meeting will be started in Teams (Taskforce Emergencies). All relevant information and findings will be described in the ticket. The priority will be defined based on the threat level and may change during the investigation.

If necessary, incidents can also be logged in the Sharepoint Logbook. [ICT - Infrastructure Service Interruptions Logbook - Report \(sharepoint.com\)](#)

The following schema explains the general process of a security incident:



CSIRT Partner Contacts

Netzwerk - Firstframe NetSec1 Support +41 41 <redacted> / Pikett +41 41 <redacted>

Netzwerk - Fortinet CSIRT FortiGuardIR@Fortinet.com / www.fortinet.com/corporate/about-us/contact-us/experienced-a-breach

Netzwerk - Swisscom CSIRT 0800 850 000