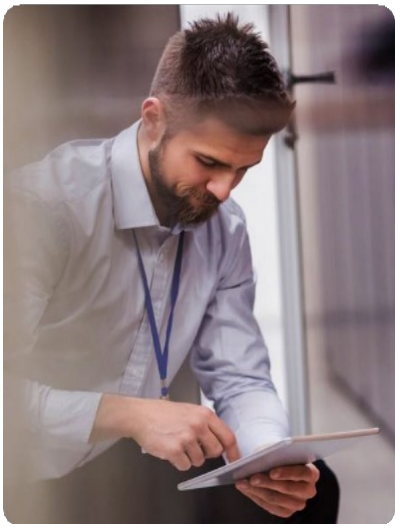
Incident Response Team

RFC 2350

The following profile of IRT has been prepared in adherence to RFC 2350, Expectations for Computer Security Incident Response.



Conscia
Secure progress

Contents

1: Document Information

1:1: Document information

Title	RFC 2350
Version	2.1
Document Date	21. January 2025
Expiration	This document is valid until superseded by a later version

1:2: Distribution List for Notifications

Changes to this document are not distributed by a mailing list. Please address questions or remarks by e-mail to: Secure-PGP-IRT(at) dubex.dk

1:3: Locations where this document may be found

The current version of this profile is always available at: Incident Response - Conscia Danmark

2: Contact Information

2:1: Name of the Team

Incident Response Team (IRT)

2:2: Address

Østbanegade 135, 2100 København Ø

2:3: Time Zone

CET, Central European Time (UTC+1, between last Sunday in October and last Sunday in March). CEST (also CET DST), Central European Summer Time (UTC+2, between last Sunday in March and last Sunday in October).

2:4: Telephone Number

+45 32830403 (24/7)

2:5: Other Telecommunication

LinkedIn: https://www.linkedin.com/company/conscia-danmark-as/?originalSubdomain=dk

2:6: Electronic Mail Adress

Incident Response Team - encrypted communication only.

Email	Secure-PGP-IRT@dubex.dk
Expire date	April 3, 2034 8:54 AM.
Thumbprint	3A1D 9C72 D83F A949 C4BE F5B5 22D7 6E28 FA30 EBE4

Dubex Incident Response Team - SMIME encrypted communication only

Email	Secure-PGP-IRT@dubex.dk
Expire date	https://securemail.dubex.dk/

For newest certificates and verification, see https://securemail.dubex.dk/

2:9: Team Members

A full list of Dubex IRT team members is not publicly available. Team members will normally identify themselves to the reporting party in an official communication regarding an incident but are not obligated to do so.

2:10: Other Information

General information about IRT is available at https://conscia.com/dk/cybersikkerhed/managed-security-services/incident-response/

2:11: Points of Customer Contact

The main point of contact to IRT to report an incident is by phone at +45 32830403. IRT mail addresses: support (at) dubex.dk.

General contact e-mail address. For other business can be addressed to info@dubex.dk.

Our regular hours (local time in respect to public holidays in Denmark) are Monday through Friday from 9 a.m. to 17 p.m. Outside normal working hours, however our Incident Hotline is available 24/7 Incident response Hotline - Conscia Danmark

3: Contact Information

3:1: Mission Statement

The mandate for our Incident Response Team (IRT) is derived from a fundamental need to uphold and fortify the cybersecurity posture of our clients. Endorsed by the board of directors, this mandate is a testament to the integral role of security incident response in our service delivery and the broad recognition of its critical importance in protecting our client's interests. The primary purpose and mission of our IRT is to provide comprehensive and expert incident response services. Our objective is to swiftly identify, mitigate, and resolve cybersecurity incidents that could potentially impact our clients' operations. The IRT mandate aligns with Conscias mission to secure our customers' business. By providing a professional incident response service, we respond to immediate security threats and build a foundation of trust and reliability with our clients. Our commitment extends beyond incident response; we are dedicated to fostering a secure digital environment where our clients are protected from malicious cyber actors

3:2: Constituency

The constituency of our Commercial IRT consultancy is diverse, catering to three main groups: incident response retainer customers, incident response walk-in customers, and the organisation itself. This broad constituency allows Conscia to offer tailored and comprehensive incident response services, addressing a wide range of cybersecurity needs

3:3: Authority

This delineation of the authority of IRT outlies the legal and operational foundation and enables decisive action in crises. The authority empowers our IRT to safeguard our clients' digital assets effectively, upholding our commitment to their cybersecurity and trust.

Our team is granted the following specific authority:

• Operational authority: To conduct incident response activities within the systems of our retainer and walk-in clients upon their authorization.

• Enforcement authority: To enforce agreed-upon security measures during incident response per contractual agreement or customer consent.

Our authority is executed with the best possible understanding of its impact on constituent systems. Actions are taken with the utmost responsibility, ensuring no additional harm is caused. Constituents are informed of potential consequences, and whenever possible, changes to their systems are made in

consultation with them, adhering to the principle of least privilege and compliance with relevant cybersecurity frameworks.

4: Policies and services

4:1: Types of Incidents and Level of Support

IRT handles various types of security incidents. The level of support depends on the type of the incident and the severity as determined solely by the IRT staff. The Incident Response Team is responsible for detecting, analysing, and mitigating security incidents within our constituency. Our IRT's key tasks include rapid incident identification, containment, eradication, and recovery. Additionally, they coordinate communication and reporting.

4:2: Co-operation, Interaction and Disclosure of Information

IRT treats all incoming information with utmost confidentiality, regardless of its priority. Sensitive or classified data is exclusively shared and stored within a secure environment, utilizing encryption when necessary. IRT leverages this information to address security incidents effectively. Distribution of this data to other teams and team members adheres strictly to relevant legislation and is based on a need-to-know basis, preferably in anonymized form. Additionally, IRT employs the Traffic Light Protocol (TLP v2.0)

4:3: Communication and Authentication

E-mail is the preferred method of communication. When the content is sensitive or requires authentication, the xxx PGP key is used for signing e-mail messages. All sensitive or confidential communication to IRT should be encrypted using the team's PGP key

4:4: Communication and Authentication

Incident response Team provides incident response services such as triage, forensics, recovery and incident management. Broadly speaking, CSIRT's services cover the containment, eradication, recovery and lessons learnt phases of incidents response. This includes the analysis, communication, coordination and support required for each phase.

- Incident Triage All incidents go through CSIRT's triage phase to determine whether the incident actually happened and its potential extent.
- Incident Coordination
- Incident Management When mandated, CSIRT will manage the incident response, that is that one of CSIRT's Incident Managers will lead the response activities and personnel assigned to the incident, including members of the CSIRT, members of the extended CSIRT, the customer personnel assigned to the incident, and third parties. This includes managing the

communications between the different response teams, the customer management team, the customer personnel, third parties, and possible law enforcement agencies. The communications are done on a need-to-know basis.

- incident Resolution CSIRT's incident response includes the search for the root cause of the incident (patient "0", initial vector of compromise, …), the tactics, techniques, and procedures (TTP) a threat actor used, the determination of the population of machines compromised or accessed, the threat actor's intent and all information relevant for the containment and eradication. Once the intent and the full 6 extent of the incident are known, CSIRT will perform all the tasks related to the complete removal of the threat actor, its tools, and accesses from the environment (eradication) and will proceed with helping the client to recover from the incident.
- Threat Hunting When indicators of compromise related to incident with the potential for a critical impact are received either from an external party or through CSIRT's investigations and responses, CSIRT will proactively engage in threat hunts for its constituency, wherever possible, unless specifically excluded in the contract.
- Digital Forensics CSIRT performs digital forensics analyses on computers, and removable media. This may be in support of an active incident, to understand the causes of a resolved incident, in support of a criminal or civil court case, in HR and internal matters, or when instructed by a LEA.
- Threat Intelligence CSIRT will research threats in order to assist an incident response, a digital forensic analysis or a threat hunt.
- "Lessons learned" debriefing At the conclusion of an incident, CSIRT may, at the request of the affected party or parties, organize a debriefing session on the "lessons learned": CSIRT will present the items noticed during the incident response process that have hindered or prevented a speedier resolution. This debriefing aims at improving the handling of future, similar incidents.

5: Disclaimers

This document does not constitute a contract between CSIRT and its constituency and should be interpreted as presenting and explaining the roles and tasks of CSIRT. As such, CSIRT assumes no liability nor obligation as arising from the provision herein.

6: Abbreviations

Abbreviation:	Definition:
IRT	Incident Response team
CERT	Computer Emergency Response Team
CEST	Central European Summer Time
CET	Central European Time
CSIRT	Computer Security Incident Response Team
DST	Daylight Saving Time