RFC 2350 Description for SK ID Solutions AS

1. Document Information

1.1. Date of Last Update

This is version 1.0, published 2020-11-16

1.2. Distribution List of Notifications

This profile is kept up-to-date in the location specified in section 1.3.

1.3. Locations where this Document May Be Found

https://www.skidsolutions.eu/upload/files/SK_SIRT_RFC2350.pdf

2. Contact Information

2.1. Name of the Team

Full Name: Security Incident Response Team, SK ID Solutions AS

Short name: SK-SIRT

2.2. Address

Pärnu mnt 141, 11314 Tallinn, Estonia

2.3. Time Zone

EET, Eastern European Time (UTC+2, between last Sunday in October and last Sunday in March)

EEST, Eastern European Summer Time (UTC+3, between last Sunday in March and last Sunday in October)

2.4. Telephone Number

+372 610 1880

2.5. Facsimile Number

N/A

2.6. Other Telecommunication

N/A

2.7. Electronic Mail Address

Incident reports should be sent to incident[A] skidsolutions . eu

2.8. Public Keys and Encryption Information

Please encrypt any sensitive information with the following SK-SIRT PGP key:

PGP KeyID: 0B1D 92E4 E734 E18D

PGP Fingerprint: CAB49EB38C2EBAF62AC73B220B1D92E4E734E18D

The key and its signature can be found at public key servers like pgp.mit.edu

2.9. Team Members

No public information is provided about SK-SIRT team members

2.10. Other Information

N/A

2.11. Point of Customer Contact

The preferred method for contacting SK-SIRT is via e-mail, incident[A] skidsolutions . eu

SK-SIRT hours of operation are generally restricted to regular business hours (09:00-17:00 EET Monday to Friday except holidays)

3. Charter

3.1. Mission Statement

The main areas of responsibility of SK-SIRT are:

Managing information security incidents related to SK ID Solutions AS and its provided services

Servicing as a single point of contact for national and foreign CERT-s and other CSIRT-s

Coordinating the response in case of incident escalation

3.2. Constituency

SK-SIRT constituency includes all services SK ID Solutions AS provides. For more details please refer to https://www.skidsolutions.eu/en/about/

3.3. Sponsorship and/or Affiliation

SK-SIRT is a security incident response team of SK ID Solutions AS

3.4. Authority

SK-SIRT coordinates the handling of security incidents involving our constituency

4. Policies

4.1. Types of Incidents and Level of Support

SK-SIRT is authorized to address all types of security incidents which occur, or threaten to occur in our constituency

The level of support given by SK-SIRT will vary depending on the type and severity of incident or issue, though in all cases some response will be made within one working day

Note that no direct support will be given to end-users, they are expected to contact respective service support

4.2. Co-operation, Interaction and Disclosure Information

SK-SIRT values the importance of operational coordination and information sharing between CERT-s, CIRT-s and other similar entities.

SK-SIRT will exchange relevant incident response related information with the aforementioned entities with the respect of its internal procedures, Estonian and EU legal frameworks

4.3. Communication and Authentication

For communication not including sensitive data plain-text email can be used, for sensitive information PGP encrypted email is preferred

For marking information sensitivity Information Sharing Traffic Light Protocol is supported

5. Services

5.1. Incident Response

SK-SIRT will define, assess and prioritize all types of information security incidents. In particular, it will provide assistance or advice with respect to the following aspects of incident management:

5.1.1. Incident Triage

Determine incident authenticity and define the impact of the incident

5.1.2. Incident Coordination

Notify relevant CERT-s and other CSIRT-s if appropriate, contact the organizations involved to start necessary measures

5.1.3. Incident Resolution

Following internal security incident management process

Collecting evidence and interpreting data, if applicable

5.2. Proactive Activities

Periodic security auditing and testing

Monitoring vulnerability management process

Continuous activity to raise security awareness within defined constituency

6. Incident Reporting forms

No incident reporting form has been developed to report incidents to SK-SIRT, please report security incidents via encrypted e-mail to contacts given in 2.7

7. Disclaimers

While every precaution will be taken in the preparation of information, notifications and alerts, SK-SIRT assumes no responsibility for errors or omissions, or for damages resulting from the use of the information contained within