Turk Telekom Cyber Security Center Computer Security Incident Response Team (henceforth TurkTelekom-CSIRT) RFC 2350 Profile

1. Document Information

This document has been prepared in accordance with RFC 2350.

1.1 Date of Last Update

This is version 1.0, published 2019/08/08.

1.2 Distribution List for Notifications

Notifications are submitted to our mailing group cert@turktelekom.com.tr. Subscription requests for this group should be sent to the owner of the mailing group. Group membership is limited to cyber security personnel.

1.3 Locations where this Document May Be Found

The current version of this CSIRT description document is available at http://www.ttyatirimciiliskileri.com.tr/en-us/socially-responsible-investing/pages/information-security.aspx

1.4 Expiration

This document remains valid until a later version is available.

2. Contact Information

2.1 Name of the Team

Official Name: Turk Telekom Cyber Security Center
Short Name: TurkTelekom-CSIRT

2.2 Address

Turk Telekom Cyber Security Center, Turk Telekom Headquarters, Aydinlikevler Mahallesi, Turgut Ozal Bulvari 06103 Altindag/ANKARA

2.3 Time Zone

GMT+3

2.4 Telephone Number

No public information will be disclosed about the team's main or emergency telephone numbers.

2.5 Facsimile Number

No public information will be disclosed about the team's facsimile number.

2.6 Other Telecommunication

None available.

2.7 Electronic Mail Address

Incident related contact should be established through cert@turktelekom.com.tr.

2.8 Public Keys and Encryption Information

TurkTelekom-CSIRT has a PGP key, whose KeyID is 99DB27BD and whose fingerprint is BF15 344E A0BB E56B 69C7 298A 06B7 5F36 99DB 27BD. The key and its signatures can be found at the usual large public keyservers.

2.9 Team Members

No public information will be disclosed about TurkTelekom-CSIRT members.

2.10 Other Information

For additional information about information security products, services and activities, please visit http://www.ttyatirimciiliskileri.com.tr/en-us/socially-responsible-

investing/pages/information-security.aspx; you can also visit https://www.turktelekom.com.tr/en/Pages/default.aspx for general information about Turk Telekomunikasyon A.S.

2.11 Points of Customer Contact

The preferred method for contacting TurkTelekom-CSIRT is via e-mail at cert@turktelekom.com.tr; e-mail sent to this address will be handled by the responsible human, or be forwarded to the appropriate person, immediately.

If it is not possible (or not advisable for security reasons) to use e-mail, TurkTelekom-CSIRT can be reached 24/7 by telephone.

TurkTelekom-CSIRT 's hours of operation are generally restricted to regular business hours (08:00-18:00 from Monday to Friday). However, emergency phone number can be used 24/7 for contacting the team.

3. Charter

3.1 Mission Statement

The purpose of TurkTelekom-CSIRT is to ensure planning and operation of corporate security systems. Ensuring the security of telecommunication systems, ensuring compliance with information security regulations, and process management for protection, reporting, and inventory creation of critical data.

3.2 Constituency

TurkTelekom-CSIRT helps ensure cyber security of Turk Telekom, the flagship of the group companies, first. Second, TurkTelekom-CSIRT supports and cooperates with group companies, TTNET A.S., Argela Yazilim ve Bilisim Teknolojileri A.S., Innova Bilisim Cozumleri A.S., Sebit Egitim ve Bilgi Teknolojileri A.S., AssisTT Rehberlik ve Musteri Hizmetleri A.S., TT Ventures Proje Gelistirme A.S., TTES Elektrik Tedarik Satis A.S., Turk Telekom International, Net Ekran, TT Satis ve Dagitim Hizmetleri A.S., TT Odeme Hizmetleri A.S., and 11818 Rehberlik ve Musteri Hizmetleri A.S., on cyber security issues.

TurkTelekom-CSIRT helps customers using cyber security services for the continuity of uninterrupted and secure access to those services.

In addition, the team collaborate with business partners, vendors, consultants, and any authorized persons or organisations on ensuring cyber security and cyber security service quality and continuity of the customers.

3.3 Sponsorship and/or Affiliation

TurkTelekom-CSIRT is a team of information security professionals. The team serves Turk Telekom’s corporate functions and reports to Turk Telekom’s Cyber Security Director, who works with the Chief Technology Officer.

3.4 Authority

TurkTelekom-CSIRT operates with authority delegated by the Cyber Security Directorate of Turk Telekomunikasyon A.S.

4. Policies

4.1 Types of Incidents and Level of Support

Information security incidents are classified as follows:
Category: Harmful Content >>> Subcategory: Spam, Content not allowed in policies
Category: Malicious Code >>> Subcategory: Virus, Worm, Ransomware, Automated Phone Call, Rootkit, Backdoor, Trojan, Spyware
Category: Reconnaissance >>> Subcategory: Scanning, Web Scanning, Sniffing, Social Engineering
Category: Vulnerabilities >>> Subcategory: Use of Known Vulnerabilities, Cross-Site Scripting, SQL Injection, Remote File Inclusion, Other Injection/Inclusion Types, Logins, Zero-Day Exploits
Category: Violations >>> Subcategory: Privileged Account Reconciliation, Login Attempts, Botnet, Brute Force, Nonprivileged Account Reconciliation, Application Reconciliation
Category: Accessibility/Availability >>> Subcategory: DDoS, Sabotage, Software/Hardware Error, Human Error
Category: Information Security >>> Subcategory: Unauthorized Access, Data Leakage, Unauthorized Interfere in Information
Category: Fraud >>> Subcategory: Unsecure Resource Usage, Copyright, Impersonation, Phishing
Category: Other >>> Subcategory: Other (all incidents that do not fall into any of the above categories are included in this category)

The following steps apply when any of the above-mentioned incidents occurs:
- Preparation
- Identification
- Containment
- Eradication
- Recovery
- Lessons Learned

4.2 Co-operation, Interaction and Disclosure of Information

In accordance with Information Management and Classification Policy issued by the organisation the privacy classes of the information and their definitions are as follows:
- Unclassified: Identifies information assets that have not yet been classified.
- General Usage: It is safe to see the information content by everyone and there is no security risk.
- Internal Usage: The content and scope of the information is only allowed to be viewed by the internal employee.
- Confidential: There is a potential for material and moral damage to the company if the content and scope of the information is viewed by unauthorized employees and persons. The information in this class should be traceable, access to this information should be controlled and restricted.
- Highly Confidential: There is a potential for serious material and moral damage to the company if the content and scope of the information is viewed by unauthorized employees and persons. For this class of information access authority must be in senior management, in certain project group members or in specific authorized persons.

After the information is classified in accordance with Information Management and Classification Policy, the disclosure of information, including incident related information,

is performed as specified in the policy. As an example, for highly confidential and confidential information classes, the information is shared only with authorized persons or units having a valid business relationship, and by using secure transmission methods it is distributed only to persons with approved access authorization. Before the information is shared with third parties, the Confidentiality Agreement is signed, which includes the responsibilities and possible sanctions.

In addition, under Information Management and Classification Policy issued by the organisation, access to, usage, storage, transfer, destruction, sharing, distribution, and labeling of highly confidential, confidential, internal usage, general usage, and unclassified information classes are defined comprehensively. By applying the necessary controls defined in the policy, confidentiality of information is ensured.

Legal considerations taken into account with regards to the information handling include The Law on the Protection of Personal Data No. 6698, and Regulation on Network and Information Security issued by Information Technologies and Communication Authority (ICTA) which is the telecommunication sector regulatory body assigned by the law.

4.3 Communication and Authentication

In view of the internal usage, and general usage information classes that TurkTelekom-CSIRT will be dealing with, telephones will be considered sufficiently secure to be used even unencrypted. Unencrypted e-mail will not be considered particularly secure, but will be sufficient for the transmission of low-sensitivity data. If it is necessary to send highly sensitive data by e-mail, PGP will be used. Network file transfers will be considered to be similar to e-mail for these purposes: sensitive data should be encrypted for transmission.

Where it is necessary to establish trust, for example before relying on information given to TurkTelekom-CSIRT, or before disclosing confidential information, the identity and bona fide of the other party will be ascertained to a reasonable degree of trust. Within Turk Telekomunikasyon A.S., and with known corporate bodies, referrals from known trusted people will suffice to identify someone. Otherwise, appropriate methods will be used, such as a search for trusted memberships, the use of WHOIS and other internet registration information, etc, along with telephone call-back or e-mail mail-back to ensure that the party is not an impostor. Incoming e-mail whose data must be trusted will be checked with the originator personally, or by means of digital signatures (PGP in particular is supported).

The use of PGP encryption is strongly advised for sensitive information. Please refer to section 2.8 for TurkTelekom-CSIRT's PGP details.

5. Services

5.1 Incident Response

Incident response includes assessing incoming reports about incidents and following up on these with others (CSIRTs, business partners, vendors, etc.).

5.1.1 Incident Triage

- Interpretation of incoming incident reports, prioritizing them, and relating them to ongoing incidents and trends.
- Determining whether an incident has really occurred, and its scope.

5.1.2 Incident Coordination

- Categorization of the incident related information (logfiles, contact information, etc.).
- Detection of root causes for incidents.
- Notification of other involved parties on a need-to-know basis.

5.1.3 Incident Resolution

- Analysis of compromised systems.
- Collecting evidence about criminal incidents.
- Elimination of the cause of a security incident (the vulnerability exploited), and its effects (for example, continuing access to the system by an intruder).
- Aid in restoring affected systems and services to their status before the security incident.
- Providing offers for improving security infrastructure.

5.2 Proactive Activities

Proactive services include:

- Information provision
- Configuration and maintenance of security tools, applications and infrastructures
- Education and training
- Product evaluation
- Security auditing or assessments
- Announcements

6. Incident Reporting Forms

Information security incidents are reported through the Information Security Incident Notification Portal accessible via intranet. If this is not possible, notifications can also be made by e-mail or telephone. Information security incidents transmitted via e-mail address or any other communication channel are processed through the Information Security Incident Notification Portal.

7. Disclaimers

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