RFC 2350

1. Document Information
This document contains a description of CERT-AM in accordance with RFC 2350.
It provides basic information about CERT-AM, its channels of communication, and its roles and responsibilities.

1.1 Date of Last Update
Version 1.0 - 04.10.2018

1.2 Distribution List for Notifications
There is no distribution list for notifications.

1.3 Locations where this Document May Be Found
The current version of this document can be found at
https://www.cert.am/rfc2350-CERT-AM.pdf

1.4 Authenticating this Document
This document has been signed with the PGP key of CERT-AM. See section 2.8 for more details

1.5 Document Identification
Title: "RFC 2350 CERT-AM"
Version: 1.0
Document Date: October 2018
Expiration: This document is valid until superseded by a later version.

2. Contact Information

2.1. Name of the Team
National Computer Emergency Response Team Armenia.
Short name: CERT-AM

2.2. Address
CERT-AM
17-3, Aram Khachatryan str.
0033 Yerevan,
Armenia

2.3. Time Zone
Time-zone: UTC/GMT +4

2.4. Telephone Number
+374 91 185 565

2.5. Electronic Mail Address
All incident reports should be sent to reports@cert.am
Use of phone for reporting incidents should be avoided as much as possible.

2.6. Other Telecommunication
None

2.7. Public Keys and Encryption Information
PGP is used for functional exchanges between CERT-AM and its Partners (incident reports, alerts, etc).

Fingerprint: B7B2 0DAB 0EBC F5F7 AB3B EFED 1A76 1881 48E4 D5DC

2.8. Team Members
The Acting Head of CERT-AM is Armen Baghdasaryan, the Deputy Head of Unit is Grigori Saghyan. The team includes 5 staff members

2.9. Other Information

2.10.
The preferred method to contact the CERT-AM team for general inquiries is to send an e-mail to the address cert@cert.am
which is monitored by a duty officer during hours of operation.

Urgent cases can be reported by phone on +374 91 185 565

Days/Hours of Operation: 10:00 to 18:00, Monday to Friday. Out of office hours operation in case of emergency.

3. Charter

3.1. Mission Statement
CERT-AM's mission is to contribute to the security of the ICT infrastructure of all Armenian institutions, bodies and agencies ('the constituents') by helping to prevent, detect, mitigate and respond to cyber-attacks and by acting as the cyber-security information exchange and incident response coordination hub for the constituents. The scope of CERT-AM's activities covers prevention, detection, response and recovery.

CERT-AM will operate according to the following key values:
- Highest standards of ethical integrity
- High degree of service orientation and operational readiness
- Effective responsiveness in case of incidents and emergencies and maximum commitment to resolve the issues
- Building on, and complementing the existing capabilities in the constituents
- Facilitating the exchange of good practices between constituents and peers
- Fostering a culture of openness within a protected environment, operating on a need-to-know basis

3.2. Constituency
Any organization using resources of Armenian Network and domain owners of the AM ccTLD.

3.3. Sponsorship and/or Affiliation
CERT-AM is sponsored by Internet Society of Armenia (www.isoc.am).

3.4. Authority
The establishment of the CERT-AM was mandated via Internet Society of Armenia decision on 1/09/2007.

4. Policies

4.1. Types of Incidents and Level of Support
All incidents are considered normal priority unless they are explicitly labelled EMERGENCY or URGENT.

4.2. Co-operation, Interaction and Disclosure of Information
CERT-AM highly regards the importance of operational cooperation and information-sharing between Computer Emergency Response Teams, and also with other organizations which may contribute towards or make use of their services.

CERT-AM operates within the confines imposed by Republic of Armenia's legislation.

4.3. Communication and Authentication
CERT-AM protects sensitive information in accordance with relevant regulations and policies within the Republic of Armenia. In particular, CERT-AM respects the sensitivity markings allocated by originators of information communicated to CERT-AM ("originator control"). Communication security (encryption and authentication) is achieved by various means: S/Mime based email encryption (SECEM), PGP or ACID or other agreed means, depending on the sensitivity level and context.

5. Services

5.1. Announcements
This service aims at providing information (e.g. on threat landscape, published vulnerabilities, new attack tools or artefacts, security/protection measures, etc.) needed to protect systems and networks.

5.2. Alerts and warnings
This service aims at disseminating information on cyber-attacks or disruptions, security vulnerabilities, intrusion alerts, computer viruses, and providing recommendations to the constituent in order to tackle the problem.

5.3. Incident Response Coordination
This service aims at the coordination of response to information security incidents in the institutions and bodies of the Republic of Armenia, in cooperation with the owners and providers of impacted parts of the respective IT infrastructure, the Armenian and international communities of Computer Emergency Response Teams and other bodies (police, courts) as appropriate.

6. Incident Reporting
Whenever possible the incidents should be reported to CERT-AM by e-mail using the address: reports@cert.am

In case of an emergency or crisis, please provide CERT-AM with at least the following information:

- Contact details and organizational information – name of person and organisation name and address, email address, telephone number;
- Short summary of the incident/emergency/crisis;
- Details of the observations that led to the discovery of the incident - scanning results (if any), an extract from the log showing the problem, etc.;
- In case there is a need to forward any emails to CERT-AM, please make sure that all email headers, body and any attachments are included.

7. Disclaimers
None