

RFC2350

aeCERT

aeCERT

One of Telecommunications and Digital Government Regulatory Authority (TDRA) Initiatives
P O Box 116688, Dubai, United Arab Emirates (UAE)
www.aecert.ae | www.tdra.gov.ae

Disclaimer

Whilst every effort has been made to ensure the accuracy of the information contained within this document, aeCERT and the TDRA bear no liability or responsibility for any recommendations issued or inadvertent damages that could be caused by the recipient of this information.

Accessing third-party links in this document will direct you to an external website. Please note that aeCERT bears no responsibility for third-party website traffic. aeCERT will have no liability to the entities for the content or use of the content available through the hyperlinks that are referenced.

1. Document Information

This document describes the aeCERT team and the services aeCERT provides based on the RFC 2350 standard.

1.1 Date of Last Update:

April 26, 2022

1.2 Distribution List for Notifications:

There is no distribution list for notifications of new versions of this document.

1.3 Locations Where This Document May Be Found:

This document is currently only available offline.

1.4 Expiration:

This document shall remain valid until replaced by a later version.

2. Contact Information

2.1 Team name:

Full name: United Arab Emirates Computer Emergency Response Team.

Short name: aeCERT

2.2 Address:

aeCERT

TDRA Dubai Office

P.O. Box 116688

Dubai, United Arab Emirates

2.3 Time Zone:

aeCERT's location is Dubai, United Arab Emirates (GMT +04:00)

2.4 Telephone Number:

Tel (+971) 4 777 4003

2.5 Email:

Incident reports should be sent to incident@aecert.ae

2.6 Public Keys and Encryption Information:

UID: aeCERT Incident Response Team incident@aecert.ae

PGP Fingerprint: 9675 1909 9ACF 0595 A3BB C166 C406 883A AD95 04A4

3. Charter

3.1 Mission statement:

The team was established to improve practices of information security, and protect the IT infrastructure in the UAE from risks and violations, in conformity with the TDRA strategy that aims at supporting and ensuring a safer cyber space for the residents of the UAE.

3.2 Constituency:

aeCERT is responsible for ensuring the information security and protection of the UAE's federal entities and the entities within the Federal network (FEDnet)

3.3 Sponsorship and/or affiliation:

The Computer Emergency Response Team (aeCERT) was established by Resolution 5/89 of 2008 issued by the Ministerial Council for Services.

3.4 Authority:

aeCERT has no legal authority over its constituents but acts as an advisory entity.

4. Policies

4.1 Types of incidents and level of support:

aeCERT provides support and advice during remediation and recovery from security incidents. aeCERT also acts as a central point to disseminate information and advice to all affected entities during high profile targeted cyber-attacks against the critical national infrastructure

Note: aeCERT follows ISO 27035 standard for Incident Management.

4.2 Co-operation, interaction and disclosure of information:

aeCERT adheres to the Traffic Light Protocol as detailed by FIRST <https://www.first.org/tlp/>. aeCERT handles all incoming information as confidential by default, but will forward the information to aid constituents in solving security incidents while adhering to the TLP classifications.

4.3 Communication and authentication:

aeCERT uses unencrypted email for general day to day activities, however, for sensitive information please refer to section 2.6.

5. Services

5.1 Incident Response:

aeCERT provides support and assistance during security incidents.

5.2 Provide Digital Forensic Analysis Services:

Forensics service includes digital forensics investigations (computer forensics and mobile device forensics), data recovery and data wiping

5.3 Provide Specialized Security Advice:

Offer recommendations with respect to the provision of specialized security advice in the field of monitoring and responding to information security incidents

5.4 Disseminate Preliminary Alerts and Advisories:

Provide proactive services in the form of preliminary alerts and advisories to constituents to improve their infrastructure and related security processes before any incident or event occurs

6. Incident Reporting Forms

Not available, please send all incident related communication to incient@aecert.ae

Contact Info



P.O. Box 116688

Dubai, United Arab Emirates

Tel (+971) 4 777 4003

Fax (+971) 4 777 4100

Email [incident\[at\]aeCERT.ae](mailto:incident[at]aeCERT.ae)

Instagram @ tdrauae

Twitter @ tdrauae

For secure communications with aeCERT with regards to sensitive or vulnerability information please send your correspondences to [incident\[at\]aeCERT.ae](mailto:incident[at]aeCERT.ae)