BGD e-GOV CIRT description, according to RFC 2350

Document date:	2018-10-23
Document version:	1.0

Table of contents

1 Document information

Document date	2018-10-23
Version date	2018-10-23
Version	1.0
Document status	Final
Author	Mohammad Ariful Islam
Reviewer	2018-10-23
Review date	2018-10-23
Document location	https://www.cirt.gov.bd/about-us/
Document authentication	PGP signature of the PDF can be found in the page https://www.cirt.gov.bd/about-us/

Chronology of versions:

Version No.	Date	Reviewed	Description
V.1.0	2018-10-23	Mohammad Ariful Islam	Final version

2   Contact Information

2.1	Name of the Team	BGD e-GOV CIRT Bangladesh e-Government Computer Incident Response Team
2.2	Address	BGD e-GOV CIRT, 12th Floor, E-14/X, ICT Tower, Agargaon, Dhaka-1207, Bangladesh
2.3	Time Zone	Bangladesh Standard Time, UTC/GMT +6h, no DST
2.4	Telephone Number	+88028181392 ext. 117, GMT+6
2.5	Facsimile Number	+88028181383
2.6	Other Telecommunication	N/A
2.7	Electronic Mail Address	cirt@cirt.gov.bd
2.8	Public Keys and Other Encryption Information	2048R/87DD5483 2015-10-07 BGD e-GOV CIRT <cirt@cirt.gov.bd> Fingerprint= F38B24C7E39C85AC5828F14A2533F28087DD5483
2.9	Team Members	Team members of BGD e-GOV CIRT are listed in Trusted introducer restricted member area. All contact information can be found in the web page https://www.cirt.gov.bd/contacts/.
2.10	Other Information	All other information about BGD e-GOV CIRT can be found in the webpage: https://www.cirt.gov.bd/about-us/
2.11	Points of Customer Contact	Preferred method for contacting BGD e-GOV CIRT is via email at cirt@cirt.gov.bd, or by using web form for incident reporting https://www.cirt.gov.bd/incident-reporting/ .

3 Charter

3.1 Mission Statement

Mission of BGD e-GOV CIRT is:

- To support government efforts to develop and amplify ICT programs by establishing incident management capabilities within Bangladesh;
- Serve as a catalyst in organizing national cybersecurity resilience initiatives (education, workforce competence, regulation, cyber exercises) among various stakeholders;
- Make efforts to establish national cyber security incident management capabilities in Bangladesh.

3.2 Constituency

Constituency of BGD e-GOV CIRT are all governmental institutions of Bangladesh.

Including but not limited to following descriptions:
- AS63932
- bcc.gov.bd
- bcc.net.bd
- 43.229.12.0/22
- 103.48.16.0/22
- 114.130.54.0/23
- 180.211.213.0/24

3.3 Sponsorship and/or Affiliation

All activities of BGD e-GOV CIRT are funded by Bangladesh government and World Bank.

3.4 Authority

BGD e-GOV CIRT operates under supervision of Executive Director of Bangladesh Computer Council.

4 Policies

4.1 Types of Incidents and Level of Support

BGD e-GOV CIRT is authorized to deal with all types of cyber security incidents which occur in constituents networks.

Level of support depends on:
- Severity of the incident;
- Importance of the system affected.

4.2	Co-operation, Interaction and Disclosure of Information	All incoming information is tagged as either a Confidential or Public. To support TLP scheme all incoming information marked as TLP:RED, TLP:AMBER or TLP:GREEN is considered as a Confidential internally. TLP:WHITE marking is tagged as a Public accordingly. Confidential information can be distributed internally on need-to-know basis according to the business needs and cannot be disclosed to third party persons who are not explicitly authorized to receive the information. It is the responsibility of the employee to take necessary measures in order to avoid unauthorized disclosure of Confidential information. Confidential information can be disclosed to the third parties on NDA basis only and with authorization of Executive Director of Bangladesh Computer Council. Public information can be released freely without any restrictions. All incoming incident related data is considered as Confidential and is handled accordingly.
4.3	Communication and Authentication	PGP is considered as a preferable and secure method to protect information. BGD e-GOV CIRT has a team key as described in 2.8. Every team member possess personal PGP key in order to exchange personal messages in secure manner.

5   Services

5.1	Reactive services	BGD e-GOV CIRT will receive information regarding cyber security incidents, triage incidents and coordinate response. Activities related to incident handling include: • Reporting • Coordination • Incident response support • Incident analysis and evidence collection
5.2	Proactive Services	• Security assessments • Configuration and maintenance of security tools, applications, infrastructures, and services • Intrusion detection • Security consulting • Awareness building

6   Incident Reporting Forms

6.1 Web form	Incident reporting form is available at the following webpage: https://www.cirt.gov.bd/incident-reporting/

7   Disclaimers

The purpose of this document is to provide a generalized overview of BGD e-GOV CIRT services.

BGD e-GOV CIRT services description provided in Memorandum of understanding (MOU) with constituents might differ from services description provided in this document. MOU always take precedence over this document.