RFC 2350

Bw-CSIRT

Version: 2 Date : Friday 4 November 2022 Author: Emmanuel Thekiso < emmanuel. thekiso(@)cirt.org.bw

Table of Contents

1. Document Information

This document contains a description of Botswana CIRT (Bw-CSIRT) accordance to RFC2350[1]. It provides basic information about Bw-CSIRT, its channels of communication, services and its role and responsibilities.

1.1 Date of Last Update

This is version 2.0, published 08-11-2022

1.2 Distribution List for Notifications

There is no distribution list for notification as of November 2022

1.3 Locations where this document may be found

https://www.cirt.org.bw/rfc-2350

1.4 Authenticating this document

This document has been digitally signed by Emmanuel Thekiso, The Head of Bw-CSIRT

1.5 Document Identification

Title	RFC2350
Version	2.0
Document Date	08 November 2022
Expiration	This document is valid until superseded by a later version

2. Contact Information

2.1 Name of the Team

Full Name	Botswana National Computer Security Incident Response Team
Short name	Bw-CSIRT

[1] http://www.ietf.org/rfc/rfc2320.txt

2.2 Address

Botswana Communications Regulatory Authority,
Plot 50671, Independence Avenue,
Gaborone,
Botswana

2.3 Time Zone

Greenwich Mean Time (GMT+2), in Central Africa Time Zone (CAT)

2.4 Telephone Number

+267-3685548, +267 3929960, +267-3957755

2.5 Facsimile Number

Not applicable

2.6 Electronic e-Mail Address

For notifications and operational matters, please contact us at: Email address: Info(@)cirt.org.bw, and for incident reporting email : ticket(@)cirt.org.bw.The email address is monitored by duty officers during hours of operations .

2.7 Other Telecommunications

N/A

2.8 Public Keys and Encryption Information

PGP key ID	0x88012C52
PGP Key Fingerprint	DAF5 2A67 B39E C7F7 F7E8 53F2 8A7F 14F8 8801 2C52

Please use this key when you want/need to encrypt messages that you send to Bw-CSIRT

2.9 Team Members

The head of Bw-CSIRT is Emmanuel Thekiso. Information about other team members is available by request.

2.10 Other Information

- General information about Bw_CSIRT is available at https://www.cirt.org.bw
- Bw-CSIRT is a member of AfricaCERT[2] .
- Bw-CSIRT complies with the CSIRT Code of Practice[3]
- Bw-CSIRT supports the use of the Information Sharing Traffic Light Protocol[4]

2.11 Days of Operation

Our days of operation are from 07:30 to 17:00 GMT+2 on business days Monday to Friday. We may operate out of these hours and days in case of emergency only.

Emergency Cases: If it's not possible to use e-mail, please call the hotline number +267-73111260 and +2673685548

3. Charter

3.1 Mission Statement

The Bw-CSIRT mission is to create, maintain, and promote the adequate capabilities for Botswana to respond to cyber threats and to protect its national critical information infrastructures. The scope of our activities covers **prevention, detection, response, and recovery**.

We operate according to the following **key values**:

- The highest standard of ethical integrity
- High degree of service orientation and operational readiness
- Fostering culture of openness within a protected environment
- Exchange of good practices among our constituents and our peers
- Effective responsiveness in case of cybersecurity incidents and emergencies at the highest level

3.2 Constituency

The Constituency of Bw-CSIRT is basically all economic sectors of Botswana as stated in the National Cybersecurity Strategy. Note that usually no direct support will be given to end users; they are expected to contact their ISPs system administrators, network administrators for assistance

[2] https://www.africacert.org/
[3] https://trustedintroducer.org/CCoPv21.pdf.
[4] https://www.first.org/tlp

3.3 Sponsorship and/or Affiliation

Bw-CSIRT is an independent organization under the Ministry of Communications, Knowledge, and Technology.

3.4 Authority

The team coordinates cybersecurity incidents on behalf of its constituency and has no authority reaching further than that. The team is however expected to make operational, non-obligatory recommendations in the course of their work. The implementation of such recommendations is not a responsibility of the team, but solely of those to whom the recommendations were made

4. Policies

4.1 Types of Incidents and Level of Support

All cybersecurity incidents will be given normal priority unless they are explicitly labelled **EMERGENCY** or **URGENT.** The Bw-CSIRT is committed to keep its constituents informed of potential vulnerabilities and existing threats before they are actively exploited. Special attention will be given to issues affecting critical infrastructure and designated operators

4.2 Co-operation, interaction, and disclosure of information

Bw-CSIRT highly regards the importance of operational cooperation and information sharing between CSIRTs and other organizations that may contribute towards or make use of the services. Bw-CSIRT cooperate with other organizations like the law enforcement agencies to protect the privacy of its constituency and stakeholders and operates within the laws of Botswana when disclosing information.

4.3 Communication and Authentication

Bw-CSIRT protects sensitive information in accordance with the relevant policies, and in particular respects the sensitivity markings defined by the originators of information. The Bw-CSIRT uses the PGP encryption and signing for secure communication.

5. Services

The Bw-CSIRT has adopted the use of **FIRST CSIRT Services Framework** [5] and provides assistance on prevention, detection, resolution and advice to its

[5] https://www.first.org/standards/frameworks/csirts/csirt_services_framework_v2.1

constituent on the following aspects of **information security incident management**

5.1 Reactive Services

- Incident Response
- Incident triage
- Cyber threat intelligence
- Alerts and warnings,
- Incident detection and resolution
- Analyzing information security incidents
- Information security incident coordination
- Supporting crisis management

5.2 Proactive Activities

The Bw-CSIRT **proactively** advises its constituency regarding recent vulnerabilities and trends in cybersecurity and includes :-

- information dissemination
- Education and awareness raising
- Training in incident management
- Cooperating with other CSIRTs
- Threats Monitoring
- Announcement about existing vulnerabilities
- Technology Watch
- Assist with development of new CSIRTs

5.3 Service Level

BW-CSIRT will always strive to react to incoming incident reports from humans within one business day. Due to current staffing levels this cannot be guaranteed, though. If you haven't received feedback to an incident report after two business days, we ask that you contact us again.

6. Incident Reporting

Incident reporting forms are not available. Please report security incidents via encrypted security(@)cirt.org.bw/ , When contacting us please provide at least the following

- Incident date and time (including time zone)
- Contact details, organizational information, name of a person, organizational name, and address, email address, telephone number

- Short summary of the incident/emergency /crisis and type of event
- The event/incident (e.g., which system produced the alert).
- Affected systems, Source IPs, ports, and protocols
- And any relevant information

7. Disclaimers

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

-

==========

END