RFC 2350
Botswana CSIRT

Version: 4.0
Date: Friday 18 September 2026
Author: Emmanuel Thekiso, emmanuel.thekiso(@)cirt.org.bw

Table of Contents

1 Document Information

This document contains a description of Botswana Computer Security Incident Response Team (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 4.0, published 11-09-2026

1.2 Distribution List for Notifications

There is no distribution list for notification as of September 2026

1.3 Locations where this document may be found

https://www.cirt.org.bw/services/rfc2350.pdf

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 Botswana CSIRT
Version	5.0
Document Date	11 September 2026
Expiration	This document is valid until superseded by a later version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 National CSIRT
Botswana Communications Regulatory Authority,
Spectrum House, Phakalane
Plot 66459, Phakalane,
Gaborone, Botswana

2.3 Time Zone

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

2.4 Telephone Number

+267-3685548, 0800

2.5 Facsimile Number

+267 3957976

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

For any other questions please contact info(@)bocra.org.bw

2.8 Public Keys and Encryption Information

PGP key ID	0xbe3be88ba4900dfd
PGP Key Fingerprint	CE8A E05F CAAF 011D 07A2 3F8A BE3B E88B A490 0DFD
Location	https://pgp.circl.lu/

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.

- **Other Information**
  General information about Bw-CSIRT is available at https://www.cirt.org.bw [2]
- Bw-CSIRT is a member of AfricaCERT[3] .
- Bw-CSIRT is an accredited member of TF-CSIRT [4]
- Bw-CSIRT is member of FIRST and comply with CSIRT Code of Practice[5].
- Bw-CSIRT supports the use of the FIRST Information Sharing Traffic Light Protocol[6].

2.10 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 0800 155 202/ 0800 1555 202 and +267-3685548. 73111260

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**.

3.2 Constituency

The Constituency of BW-CSIRT is listed in the Cybersecurity ACT [7].

[2] https://www.cirt.org.bw
[3] https://www.africacert.org/
[4] https://www.trusted-introducer.org
[5] https://www.first.org/about/policies/code-of-conduct
[6] https://www.first.org/tlp

[7] https://www.cirt.org.bw/cybersecurity_act

3.3 Sponsorship and/or Affiliation

BW-CSIRT is an independent organization under the National Cybersecurity Authority (NCA)[8], hosted under the Botswana Communications Regulatory Authority (BOCRA)

3.4 Authority

BW-CSIRT main purpose is to help coordination amongst local incident response initiatives to handle any kind of incidents at constituency level based on terms and conditions within the Non-disclosure Agreement (NDA). This includes communication with counterparts and initiates collaboration.

4 Policies

4.1 Types of Incidents and Level of Support

Bw-CSIRT is authorized to address any kind of cybersecurity incidents, which occur or threaten our constituency. We will impose any precaution action needed and committed to keeping our constituency informed to any potential vulnerability. The level of support given by Bw-CSIRT depends on the type and severity of the incident. Special attention will be given to an event that is directly affecting members and constituency's critical infrastructure. ***Please note that no direct user support will be given to end users***. Users are expected to contact their local ISP security team or, network administrator for assistance.

4.2 Co-operation, interaction, and disclosure of information

Bw-CSIRT cooperates with other organizations in the field of cybersecurity resilience and Internet infrastructure. BW-CSIRT is committed to protect the privacy of its constituency and only pass on limited and anonymized information to other parties, unless some contractual agreements apply, for example, Non-Disclosure Agreement (NDA).

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.

[8] https://www.cirt.org.bw/cybersecutity_act /

/

4.3 Communication and Authentication

BW-CSIRT protects sensitive information in accordance with the relevant policies. 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** [9] and provides assistance on security incidents prevention, detection, resolution and advice to its constituency.

5.1 Service Level

BW-CSIRT will always strive to react to incoming incident reports within one business day.

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:

a) Incident date and time (including time zone)
b) Contact details, organizational information, name of a person, organizational name, and address, email address, telephone number
c) Short summary of the incident/emergency /crisis and type of event
d) The event/incident (e.g., which system produced the alert)
e) Affected systems, Source IPs, ports, and protocols
f) And any relevant information

7 Disclaimers

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

---------- END ……..

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