




Company Confidential

This document, its contents and intellectual property, belongs to Botswana Communications Regulatory Authority and may not be disclosed to any party without prior written consent.



Botswana National CSIRT

Baseline Security requirements for Services Providers

| | |
|--------------------|---|
| Produced By | Botswana Communications Regulatory Authority |
| Document Custodian | |
| Revision No. | |
| Signature |  |
| Date | 04 November 2025 |

| Document Name | Revision | Print Date | Page |
|--------------------------------|----------|---------------|---------|
| Baseline Security Requirements | 1.0 | DRAFT12112024 | 1 of 14 |

Table of Contents

| | |
|---|----|
| 1. Introduction..... | 3 |
| 2. Scope..... | 3 |
| 3. International Standards & Framework..... | 4 |
| 4. Confidentiality and Data Protection..... | 4 |
| 5. Information Security Practices:..... | 5 |
| 6. Access Controls:..... | 5 |
| 7. Security Incident Reporting and Response..... | 6 |
| 8. Compliance with Security Policies and Standards..... | 6 |
| 9. Security Audits and Inspections:..... | 7 |
| 10. Subcontractor Management..... | 7 |
| 11. Technology Clauses..... | 8 |
| 12. Software Security..... | 8 |
| 13. Encryption and Secure Communications:..... | 8 |
| 14. Secure Development and Deployment Practices:..... | 9 |
| 15. Vulnerability Management:..... | 9 |
| 16. Secure Cloud Services (if applicable):..... | 10 |
| 17. Security Testing and Assurance:..... | 10 |
| 18. Non-Technology Clauses..... | 11 |
| 19. Physical Security:..... | 11 |
| 20. Personnel Security..... | 11 |
| 21. Secure Handling and Disposal..... | 12 |
| 22. Third-Party Service Providers:..... | 12 |
| 23. Security Awareness and Training..... | 13 |
| 24. Incident Response and Reporting..... | 13 |
| 25. Business continuity & disaster recovery..... | 14 |

| Document Name | Revision | Print Date | Page |
|--------------------------------|----------|---------------|---------|
| Baseline Security Requirements | 1.0 | DRAFT12112024 | 2 of 14 |

Introduction

- a. The Computer Incident Response Team (CSIRT) which currently operates under BOCRA has the objective to promote a safe cyber space. To achieve this, the CSIRT’s role is to ensure information security through proactive and reactive services including threat monitoring, incident handling, threat intelligence, and cyber awareness. Although the CSIRT serves National Critical Infrastructure (NCII) as identified by NCS, its specific focus on Licensees (Service Providers) takes advantage of established licensee and compliance requirements, including Business Continuity Guidelines.
- b. Recent cybersecurity incidents in Botswana have severely impacted the operations of several companies, highlighting the need for baseline cybersecurity requirements for critical sectors including the communications industry. While the CSIRT will provide cybersecurity guidance through these guidelines, as well as advisories, service providers will ensure compliance and adherence to baseline cybersecurity requirements.
- c. This document establishes these requirements for Service Providers, promoting the implementation of enhanced security measures to safeguard networks, systems, and consumers.

1. Scope

- a. The baseline cybersecurity requirements, covers all Services Providers licensed by BOCRA. These Guidelines may also apply to other Critical Information Infrastructure belonging to sectors identified as critical in the NCS.

| Document Name | Revision | Print Date | Page |
|--------------------------------|----------|---------------|---------|
| Baseline Security Requirements | 1.0 | DRAFT12112024 | 3 of 14 |

2. International Standards & Framework

Constituents are encouraged to review international standards and frameworks to enhance infrastructure protection and align their controls based on them. The Baseline Cybersecurity Requirements are based on the following:

- a. ISO/IEC 27001:2013: Requirements for establishing, implementing, maintaining, and improving an information security management system.
- b. ITU-T Rec X.1051, 2016: Security techniques code of practice for telecommunications organizations based on ISO/IEC 27002.
- c. NIST Framework, Version 1.1, 2018: Framework for improving critical infrastructure cybersecurity, including; Identify, Protect, Detect, Respond, and Recover functions.
- d. ENISA Technical Guidance on Security Measures, Version 2, 2014: Guidance with seven security domains and twenty-five high-level security objectives.

3. Confidentiality and Data Protection:

- a. The Service Provider shall treat all data including but not limited to personal data, intellectual property, and confidential business information, as strictly confidential and shall not disclose, share, or use such data and information for any purpose other than the performance of its obligations under this agreement.
- b. The Service Provider shall implement and maintain appropriate technical, physical, and organizational measures to protect the confidentiality, integrity, and availability of its data and information, in accordance with industry best practices and applicable laws and

| Document Name | Revision | Print Date | Page |
|--------------------------------|----------|---------------|---------|
| Baseline Security Requirements | 1.0 | DRAFT12112024 | 4 of 14 |

regulations, including but not limited to relevant laws/regulations such as data protection law.

- c. The Service Provider shall ensure that all personnel who have access to its data and information are bound by appropriate confidentiality obligations and receive regular training on data protection and security practices.

4. Information Security Practices:

- a. The Service Provider shall implement and maintain an Information Security Management System (ISMS) that complies with industry-recognized standards, such as ISO 27001 or NIST Cybersecurity Framework.
- b. The Service Provider shall regularly assess and mitigate risks to the security of its data and information, including but not limited to risks arising from cyber threats, human errors, and natural disasters.
- c. The Service Provider shall implement and maintain appropriate security controls, including but not limited to access controls, network security, malware protection, secure configurations, and security monitoring and logging.

5. Access Controls:

- a. The Service Provider shall implement and maintain strict access controls, including but not limited to multi-factor authentication, least privilege principles, and regular review of access rights, to ensure that only authorized personnel have access to the organisation data and information, on a need-to-know basis.

| Document Name | Revision | Print Date | Page |
|--------------------------------|----------|---------------|---------|
| Baseline Security Requirements | 1.0 | DRAFT12112024 | 5 of 14 |

- b. The Service Provider shall maintain detailed logs of all access to the organisation data and information and make such logs available to BOCRA upon request for auditing and monitoring purposes.

6. Security Incident Reporting and Response:

- a. The Service Provider shall establish and maintain an incident response plan to promptly detect, respond to, and mitigate security incidents and data breaches.
- b. The Service Provider shall promptly report any actual or suspected security incidents, data breaches, or unauthorized access to the BOCRA within 24 hours and provide regular updates on the investigation and remediation efforts.
- c. The Service Provider shall cooperate fully with the BOCRA (CSIRT) in the investigation and resolution of any security incidents or data breaches and shall take all necessary steps to mitigate the potential harm and prevent future occurrences.

7. Compliance with Security Policies and Standards:

- a. The Service Provider shall comply with CSIRT's information security policies, procedures, and standards, as provided and updated from time to time.
- b. The Service Provider shall ensure that its services, products, and systems comply with relevant industry standards and best practices for information security, such as specify relevant standards, e.g., Data Protection Act.

| Document Name | Revision | Print Date | Page |
|--------------------------------|----------|---------------|---------|
| Baseline Security Requirements | 1.0 | DRAFT12112024 | 6 of 14 |

8. Security Audits and Inspections:

- a. BOCRA (CSIRT) reserves the right to conduct security audits, assessments, and inspections of the Service Providers' systems, processes, facilities, and personnel involved in the handling of Organisations data and information, to ensure compliance with the agreed security requirements.
- b. The Service Provider shall cooperate fully with BOCRA and provide all necessary information, access, and assistance to facilitate such audits and inspections.
- c. The Service Provider shall promptly remediate any identified security deficiencies or non-compliances within a reasonable period agreed upon with BOCRA.

9. Subcontractor Management:

- a. If the Service Provider engages any subcontractors or third-party service providers to perform services involving the handling of its data and information, the Service Provider shall ensure that such subcontractors or third parties comply with the same security requirements and obligations as set forth in this Agreement.
- b. The Service Provider shall remain fully responsible and liable for the acts and omissions of its subcontractors or third-party service providers concerning the security and protection of its data and information.

| Document Name | Revision | Print Date | Page |
|--------------------------------|----------|---------------|---------|
| Baseline Security Requirements | 1.0 | DRAFT12112024 | 7 of 14 |

10. Technology Clauses

Software Security:

- a. The Service Provider shall implement secure software development practices, including but not limited to secure coding techniques, code reviews, static and dynamic code analysis, and security testing throughout the software development life cycle (SDLC).
- b. The Service Provider shall promptly address and remediate any identified software vulnerabilities or security flaws within a reasonable period agreed upon with the CSIRT.
- c. The Service Provider shall provide BOCRA with detailed information about the security architecture, design, and implementation of the software, including security controls, encryption mechanisms, and data flow diagrams.

11. Encryption and Secure Communications:

- a. The Service Provider shall use industry-standard encryption protocols and encryption standards, e.g., AES-256, TLS 1.3, or higher for transmitting service providers data and information.
- b. The Service Provider shall implement secure communication channels, such as secure file transfer protocols (SFTP) or virtual private networks (VPNs), Pretty Good Protocols (PGP) and Traffic Light Protocols (TLP) as recommended by Forum of Incident Response and Security Teams (FIRST) for the exchange of sensitive data and information with CSIRTs.
- c. The Service Provider shall maintain and regularly update digital certificates, encryption keys, and other cryptographic materials used for securing communications and data.

| Document Name | Revision | Print Date | Page |
|--------------------------------|----------|---------------|---------|
| Baseline Security Requirements | 1.0 | DRAFT12112024 | 8 of 14 |

12. Secure Development and Deployment Practices:

- a. The Service Provider shall follow secure software development life cycle (SDLC) practices, including but not limited to requirements analysis, secure design, secure coding, code reviews, testing, and secure deployment processes.
- b. The Service Provider shall implement secure configuration management practices, including version control, change management, and separation of environments (development, testing, and production).
- c. The Service Provider shall maintain detailed documentation of the software development and deployment processes, including security controls, configurations, and changes made throughout the SDLC.
- d. When hosting domains and/or web applications, Service providers should ensure compliance with the .bw ccTLD policies including the Registrar Accreditation Agreement, Registration Terms and Conditions, as well as the Acceptable Use Policy among others.
- e. Separate Web Application Security Guidelines are provided as an annexure to this document.

13. Vulnerability Management:

- a. The Service Provider shall implement a vulnerability management program that includes regular vulnerability scanning, risk assessment, and timely patching of identified vulnerabilities in the software, systems, and supporting infrastructure.

| Document Name | Revision | Print Date | Page |
|--------------------------------|----------|---------------|---------|
| Baseline Security Requirements | 1.0 | DRAFT12112024 | 9 of 14 |

- b. The Service Provider shall maintain an up-to-date inventory of all software components, libraries, and dependencies used in the software, and monitor for and address any security vulnerabilities or updates in a timely manner.
- c. The Service Provider shall provide BOCRA with detailed reports on identified vulnerabilities, risk assessments, and remediation plans, and shall obtain BOCRA's approval before implementing any high-risk patches or updates for advice.

14. Secure Cloud Services:

- a. Service Provider offering cloud services must implement adequate security measures, including logical data separation, secure multi-tenancy, role-based access controls, and compliance with relevant cloud security standards and best practices.
- b. The Service Provider shall provide detailed information about the cloud architecture, security controls, data segregation mechanisms, and redundancy measures implemented to ensure the security and availability of data and systems hosted in the cloud.
- c. The Service Provider must ensure that all data and information it owns is stored and processed within the agreed-upon geographic regions. Any cross-border data transfers require prior approval.

15. Security Testing and Assurance:

- a. The Service Provider shall conduct regular security testing, including but not limited to penetration testing, vulnerability scanning, and security code reviews, to identify and address potential security weaknesses or vulnerabilities in the software, systems, and supporting infrastructure.

| Document Name | Revision | Print Date | Page |
|--------------------------------|----------|---------------|----------|
| Baseline Security Requirements | 1.0 | DRAFT12112024 | 10 of 14 |

- b. The Service Provider shall provide the CSIRT with detailed reports on the security testing activities, findings, and remediation plans, and shall obtain the CSIRT's approval before implementing any high-risk remediation actions.
- c. The Service Provider shall engage independent third-party security assessments or audits, as requested by BOCRA, to validate the effectiveness of the security controls and measures implemented.

16. Non-Technology Clauses

Physical Security:

- a. The Service Provider shall implement appropriate physical security measures to protect its data and information from unauthorized access, theft, or damage, including but not limited to access controls, video surveillance, intrusion detection systems, and secure storage facilities.
- b. The Service Provider shall ensure that all physical documents, media, and equipment containing data and information are stored in secured areas with restricted access and appropriate environmental controls (e.g., temperature, humidity, fire suppression).
- c. The Service Provider shall maintain detailed logs of all physical access to areas data and information are stored or processed and make such logs available to BOCRA upon request for auditing and monitoring purposes.

Personnel Security:

- a. The Service Provider shall conduct background checks, including criminal record checks and employment verification, on all personnel who will have access to its data and information, in accordance with applicable laws and regulations.

| Document Name | Revision | Print Date | Page |
|--------------------------------|----------|---------------|----------|
| Baseline Security Requirements | 1.0 | DRAFT12112024 | 11 of 14 |

- b. The Service Provider shall ensure that all personnel who have access to the data and information receive regular security awareness training, covering topics such as data protection, handling of sensitive information, and incident reporting procedures.
- c. The Service Provider shall ensure that all personnel who have access to the data and information are bound by appropriate confidentiality agreements and be aware of their obligations to protect the confidentiality, integrity, and availability of such data and information.

17. Secure Handling and Disposal:

- a. The Service Provider shall implement secure handling procedures for any physical documents or media containing its data and information, including but not limited to secure transportation, handling, and storage practices.
- b. The Service Provider shall implement secure disposal procedures for any physical documents or media containing its data and information, such as shredding, degaussing, or secure erasure, to ensure that the data and information cannot be recovered or reconstructed.
- c. The Service Provider shall maintain detailed logs of all handling and disposal activities related to its data and information and make such logs available upon request for auditing and monitoring purposes.

18. Third-Party Service Providers:

- a. If the Service Provider engages any third-party service providers or subcontractors to perform services involving the handling of data and information, the Service Provider shall ensure that such third

| Document Name | Revision | Print Date | Page |
|--------------------------------|----------|---------------|----------|
| Baseline Security Requirements | 1.0 | DRAFT12112024 | 12 of 14 |

parties comply with the same security requirements and obligations as set forth in these Guidelines.

- b. The Service Provider shall conduct due diligence on any third-party service providers or subcontractors to assess their security practices, certifications, and compliance with relevant standards and regulations.
- c. The Service Provider shall remain fully responsible and liable for the acts and omissions of its third-party service providers or subcontractors concerning the security and protection of data and information.

19. Security Awareness and Training:

- a. The Service Provider shall provide regular security awareness and training programs to all personnel involved in the handling of the data and information, covering topics such as data protection, incident response, secure handling and disposal procedures, and relevant security policies and procedures.
- b. The Service Provider shall maintain detailed records of security awareness and training activities, including attendance logs, training materials, and assessments, and make such records available to BOCRA upon request for auditing and monitoring purposes.

20. Incident Response and Reporting:

- a. The Service Provider shall establish and maintain an incident response plan to promptly detect, respond to, and mitigate security incidents and data breaches involving BOCRA's data and information.

| Document Name | Revision | Print Date | Page |
|--------------------------------|----------|---------------|----------|
| Baseline Security Requirements | 1.0 | DRAFT12112024 | 13 of 14 |

- b. The Service Provider shall promptly report any actual or suspected security incidents, data breaches, or unauthorized access to CSIRT or information systems within 24 hours and provide regular updates on the investigation and remediation efforts.
- c. The Service Provider shall cooperate fully with BOCRA CSIRT in the investigation and resolution of any security incidents or data breach.

21. Business Continuity & Disaster Recovery

- a. In the event of a cybersecurity incident, service providers must have a comprehensive Business Continuity Plan (BCP) and Disaster Recovery Plan (DRP) in place to ensure uninterrupted delivery of essential services.
- b. The BCP and DRP should cover various cybersecurity threat scenarios and be reviewed annually to ensure their effectiveness and relevance.
- c. CII Operators must have robust restoration and backup plans to recover critical assets in case of system disruptions, data corruption, or cyber-attacks. Backup copies of data, software, and systems should allow for data restoration to an earlier state in such situations.
- d. CII Service Providers must conduct periodic backups according to the organization's operational needs to ensure successful completion.
- e. Backups should be stored offline on devices that are not connected to any computer or the internet and should be kept separate from the corresponding CII assets.

| Document Name | Revision | Print Date | Page |
|--------------------------------|----------|---------------|----------|
| Baseline Security Requirements | 1.0 | DRAFT12112024 | 14 of 14 |