Jobu Information Security Policy

Version: 1.0
Last Reviewed: 12/03/2026

1. Introduction

Jobu Africa, a platform operated under **Broadband Communication Networks Limited (BCNL)**, facilitates connections between customers and qualified technicians, engineers, and service professionals through a digital platform.

Protecting the confidentiality, integrity, and availability of information handled through the Jobu platform is critical to maintaining user trust, operational stability, and regulatory compliance.

This Information Security Policy establishes a framework for safeguarding organizational information, platform data, and system infrastructure. The policy supports compliance with applicable legal, regulatory, and contractual requirements while promoting responsible management of digital and operational information.

All individuals who access Jobu systems or handle Jobu-related data share responsibility for protecting that information.

---

2. Purpose

The purpose of this policy is to:

- Protect sensitive information relating to Jobu operations, platform users, and business partners.
- Ensure that all personnel understand how to identify and report information security incidents.
- Establish procedures for managing and documenting security incidents.
- Minimize risks associated with data breaches, unauthorized access, or system misuse.
- Support the secure operation of the Jobu platform and associated digital infrastructure.

---

3. Scope

This policy applies to:

- Jobu employees and management
- BCNL personnel supporting Jobu operations
- contractors, consultants, and temporary staff
- service providers and vendors with access to Jobu systems or data
- third-party technology partners supporting the platform

The policy covers **all forms of information**, including:

- electronic data stored on servers or cloud infrastructure
- platform user data
- business documentation

- communications (email, messaging, and verbal discussions)
- physical records containing sensitive information

---

4. Roles and Responsibilities

Information Security Officer

Responsible for overseeing implementation, monitoring compliance, and coordinating responses to information security incidents.

Management

Managers are responsible for ensuring that team members comply with this policy and receive appropriate guidance on information security practices.

Employees and Contractors

All personnel must:

- follow established information security procedures
- protect sensitive platform and company information
- report suspected or confirmed security incidents promptly

Managing Director

The Managing Director ensures organizational processes align with this policy and that corrective actions are taken in cases of non-compliance.

---

5. Identifying Information Security Incidents

An information security incident involves the **loss, misuse, unauthorized access, or compromise of data or systems associated with Jobu operations**.

This includes incidents affecting:

- platform user information
- internal company information
- platform systems or infrastructure
- partner or vendor data

Information security incidents may occur due to:

- failure to follow security procedures
- loss or theft of devices containing data
- unauthorized access to platform accounts
- system vulnerabilities or hacking attempts
- malware or virus infections

- human error
- social engineering or phishing attacks

---

6. Examples of Information Security Incidents

Examples include, but are not limited to:

- theft or loss of laptops, mobile devices, or storage media containing company data
- unauthorized access to Jobu platform accounts or administrative systems
- accessing or sharing user data without authorization
- leaving confidential information exposed or unattended
- disclosure of passwords or login credentials
- improper disposal of confidential records
- sending sensitive information to the wrong recipient
- unauthorized use of platform data for personal or commercial gain
- attempts to manipulate platform systems or compromise security

These incidents can lead to serious consequences including:

- threats to user privacy and safety
- regulatory penalties or legal liability
- financial losses
- operational disruption
- reputational damage

---

7. Procedure for Reporting Information Security Incidents

All information security incidents must be reported **immediately upon discovery**.

Incidents should be reported to the **IT Support Team** via:

Email: itsupport@broadcom.co.ke

Prompt reporting enables the organization to assess risks and take appropriate corrective action.

Where an incident involves the loss of equipment or devices containing Jobu data, this must also be reported to the ICT service desk immediately.

---

8. Incident Documentation and Investigation

All reported incidents must be formally recorded using an **Incident Report Form**.

The individual responsible for identifying the incident must:

1. Complete the incident report form.
2. Submit the form to their line manager.

3. Ensure the completed report is forwarded to the IT Manager within **two working days**.

The incident report serves as an official record for investigation and follow-up actions.

Where the incident involves company equipment, replacement of the equipment will not occur until a completed and approved incident report has been submitted.

---

9. Incidents Involving Third Parties

If an information security incident involves a **contractor, vendor, or technology partner**, the issue must be reported through the relevant Jobu or BCNL contact responsible for managing that relationship.

The responsible team must review whether:

- contractual security obligations were met
- appropriate safeguards were in place
- corrective action is required

Where necessary, legal guidance may be sought to determine appropriate actions.

---

10. Organizational Management of Security Incidents

The IT team will maintain a **central log of all information security incidents**.

Regular reviews will be conducted to:

- identify patterns or recurring issues
- assess operational risks
- strengthen preventive controls

In accordance with BCNL's risk management practices, each incident will undergo a **risk assessment** to evaluate:

- severity of impact
- likelihood of recurrence
- necessary corrective actions

Incidents with **medium or high risk ratings** will be escalated to senior management and Human Resources where appropriate.

---

11. Disciplinary and Legal Action

Failure to comply with this Information Security Policy may result in disciplinary action.

Serious violations or repeated breaches may lead to:

- suspension of system access
- termination of employment or contract
- legal action where applicable

Where an incident involves criminal activity or illegal conduct, the matter may be reported to relevant authorities.

---

12. Further Guidance

Additional information security practices and procedures are documented in the **Information Security Handbook** and related company policies.

For any information security questions or concerns, personnel should contact:

IT Security Support
Email: itsupport@broadcom.co.ke