



JHR GENERAL SUPPLIER COMPANY LIMITED

P.O. Box 2310

Morogoro (M), Tanzania

Email: info@jhrgeneralsupplier.co.tz | johansen.herman@jhrgeneralsupplier.co.tz | jhrgeneralsupplier@gmail.com

Website: www.jhrgeneralsupplier.co.tz

Mobile: 0714 911 453 | 0783 113 700 | 0754 321 990 | 0784 664 027

Cybersecurity Policy

JHR General Supplier Company LIMITED

Effective Date: January 1, 2025

Approved by: YASSIN YUSFU MASHUUBU

Version: 1.0

Next Review Date: January 1, 2026

1. Purpose

The purpose of this Cybersecurity Policy is to outline the guidelines and responsibilities for protecting **JHR General Supplier Company LIMITED's** information technology systems, digital assets, and data from unauthorized access, cyberattacks, misuse, and data breaches.

Cybersecurity is a shared responsibility. This policy ensures that employees, contractors, and third-party users understand their role in maintaining secure and reliable IT systems.

2. Scope

This policy applies to:

- All employees, contractors, consultants, interns, and third-party service providers
- All IT systems, devices, networks, and digital platforms used to access company information
- All locations where JHR systems and data are accessed, including remote and mobile work

3. Policy Statement

JHR General Supplier Company LIMITED is committed to:

- Safeguarding the confidentiality, integrity, and availability of its information systems
- Preventing unauthorized access to sensitive company or client data
- Ensuring business continuity through effective cybersecurity measures
- Complying with applicable data protection laws and standards (e.g. GDPR, ISO/IEC 27001)

4. Key Principles

- Access to information must be limited based on business needs and roles
- Users must authenticate securely using passwords or multi-factor authentication (MFA)
- All software and systems must be kept up to date and patched against known vulnerabilities
- Cybersecurity incidents must be reported immediately and investigated promptly
- Employees must receive regular cybersecurity awareness training

5. User Responsibilities

All users must:

- Use strong, unique passwords and change them regularly
- Lock their devices when unattended
- Avoid clicking suspicious links or downloading unknown attachments
- Refrain from sharing login credentials or using unauthorized devices
- Back up data in accordance with IT guidelines
- Report all suspected security incidents or breaches immediately

6. Acceptable Use

Users may only use JHR's IT resources for **authorized business purposes**. The following are strictly prohibited:

- Installing unapproved software or hardware
- Using company devices for illegal or inappropriate activities
- Accessing restricted systems or confidential information without authorization
- Using unsecured public Wi-Fi for sensitive company transactions without a VPN
- Sharing internal data through unsecured cloud services or personal accounts

7. Data Protection and Privacy

- Sensitive data must be encrypted during storage and transmission
- Personal data must be handled in compliance with relevant data protection laws (e.g. GDPR)
- All devices accessing sensitive data must have antivirus and encryption enabled
- Portable media (e.g. USBs) must be encrypted or disabled unless authorized by IT

8. Network and System Security

- Firewalls, antivirus software, and intrusion detection systems (IDS) must be active on all networks
- Remote access must be secured with VPN and MFA
- Wireless networks must be password-protected and configured securely
- Regular system scans and penetration tests will be conducted by IT

9. Incident Response and Reporting

All cybersecurity incidents must be reported immediately to:

- **IT Department:** [Insert Contact Info]
- **Cybersecurity Officer:** [Insert Contact Info]

Examples of incidents:

- Suspected phishing or malware attacks
- Lost or stolen devices containing company data
- Unauthorized access attempts

- Data leaks or exposure of sensitive information

The IT team will:

1. Investigate the incident
2. Contain and mitigate the threat
3. Notify management and affected stakeholders
4. Document and implement corrective actions

10. Training and Awareness

- All employees must complete **annual cybersecurity training**
- New hires will receive cybersecurity orientation during onboarding
- Refresher training will be issued in response to major threats or changes in systems

11. Monitoring and Compliance

- The IT department reserves the right to monitor systems and networks to enforce policy compliance
- Random audits may be conducted to check for vulnerabilities or misuse
- Failure to comply may result in disciplinary action, including termination

12. Policy Review

This policy will be reviewed **annually** or as needed in response to:

- Changes in technology or threat landscape
- Regulatory updates
- Significant security incidents

13. Related Policies

- Acceptable Use Policy
- Data Protection and Privacy Policy
- Business Continuity and Disaster Recovery Policy
- Remote Work Policy

14. Contact Information

IT & Cybersecurity Department

JHR General Supplier Company LIMITED

Email: jhrgeneralsupplier@gmail.com , info@jhrgeneralsupplier.co.tz

website : www.jhrgeneralsupplier.co.tz

Phone: +255784664027

Office Address: street old dar es salaam road, Plot number 97 ,zone (ii) ,Brock number 103, Pamba house,Morogoro district, (CBD), Morogoro Municipal

All employees and contractors are required to read, understand, and sign an acknowledgment of this policy during onboarding and annually.