Ngwerema Close No 5, Olympia Park
Lusaka, Zambia
WEB: www.corelink.co.zm
MAIL: info@corelink.co.zm
CEL: +260963493849 / +260972615221

Information Security Policy

Submitted by:
Corelink Consulting Ltd.
PACRA Registration Number: 120220026085
Ngwerema Road No. 5, Olympia Park
Lusaka, Zambia

Document Version: 1.0

Prepared For: Client Software Development Projects
Date: February 18, 2025

Table of Contents

1. Introduction and Purpose

Corelink Consulting Limited ("Corelink," "the Company") has established this Information Security Policy to safeguard its information assets against a wide range of security threats. These threats may originate from internal or external sources and can be either deliberate or accidental in nature. The procedures and guidelines set forth in this policy are designed to mitigate risks and protect the organization's sensitive information.

The primary objectives of this policy are to maintain the confidentiality, integrity, and availability of all information systems and data managed by Corelink. Additionally, the policy ensures that Corelink complies with all applicable legal, regulatory, and contractual obligations, including adherence to the Data Protection Act of Zambia.

2. Scope

This policy applies to all employees, contractors, and other third parties who have access to Corelink's information systems and data. It covers all information, regardless of its form or the medium on which it is stored, including but not limited to electronic data, paper documents, and intellectual property.

3. Roles and Responsibilities

- **Management:** Management is responsible for ensuring that this policy is implemented and enforced throughout the organization.
- **IT Staff:** The IT **Staff** is responsible for the day-to-day management and maintenance of Corelink's information security systems.
- **All Employees:** All employees are responsible for understanding and complying with this policy in their daily work.

4. Data Classification

Corelink classifies data into the following categories to ensure the appropriate level of protection is applied:

- **Public:** Information that can be freely shared with the public.
- **Internal:** Information that is intended for internal use only and should not be shared outside the company without authorization.
- **Confidential:** Sensitive information that, if disclosed, could cause significant harm to Corelink or its clients. This data requires the highest level of protection.
- **Sensitive Personal Data:** As defined by the Data Protection Act of Zambia, this includes data revealing a person's race, health status, religious beliefs, political opinions, etc. and is subject to the strictest controls.

5. Acceptable Use of Assets

All of Corelink's information technology assets, including computers, networks, and software, are to be used for business purposes only. Incidental personal use is permitted but should not interfere with employee productivity or consume significant resources.

6. Access Control

Access to Corelink's information systems is granted on a "need-to-know" basis.

- **Multi-Factor Authentication (2FA):** All systems containing confidential or sensitive personal data require two-factor authentication for access. This includes, but is not limited to, email, VPN, and access to our secure document repositories.
- **Password Policy:** All passwords must meet a minimum complexity requirement and be changed on a regular basis.

7. Data Handling and Transmission

Corelink has established secure methods for handling and transmitting sensitive information:

- **Secure Internal Document Repository:** All internal documents are stored in a secure, access-controlled repository. Access is logged and monitored.
- **Sharepoint:** For collaborative work and sharing of sensitive information with clients, dedicated and access-restricted Sharepoint sites are to be used.
- **Internal Offline NAS:** An offline Network Attached Storage (NAS) device is used for backing up and archiving highly sensitive data. Access to this device is physically and logically restricted.
- **SCIF (Sensitive Compartmented Information Facility):** For projects requiring the highest level of security, a designated SCIF is available. All activities within the SCIF are strictly monitored and controlled.

8. Data Encryption

To protect data from unauthorized access, Corelink employs the following encryption measures:

- **Encryption at Rest:** All servers, including those hosting our document repositories and databases, utilize full-disk encryption to protect data when it is not in use.
- **Encryption in Transit:** All data transmitted over public networks is encrypted using industry-standard protocols (e.g., TLS, SSL).

9. Device Management

All company-owned devices are managed through Active Directory (AD). This allows for:

- **Centralized policy enforcement:** Security policies, such as password requirements and screen lock settings, are enforced across all devices.
- **Software and patch management:** All devices receive timely security updates and patches.
- **Remote wipe capabilities:** In the event a device is lost or stolen, it can be remotely wiped to prevent data loss.

10. Compliance with the Data Protection Act of Zambia

Corelink is committed to complying with all provisions of the Data Protection Act of Zambia. This includes:

- **Lawful Basis for Processing:** We will only process personal data where we have a lawful basis to do so.
- **Data Subject Rights:** We will respect the rights of data subjects, including the right to access, rectify, and erase their personal data.
- **Data Retention:** We will not retain personal data for longer than is necessary for the purpose for which it was collected.
- **Data Protection Officer:** A Data Protection Officer has been appointed to oversee our compliance with the Act.

11. Incident Response

In the event of a security incident, Corelink will follow its established Incident Response Plan to contain the incident, mitigate its impact, and notify the relevant authorities and affected individuals as required by law.

12. Policy Review and Updates

This policy will be reviewed and updated on an annual basis, or more frequently if there are significant changes to our security posture or the regulatory environment.

13. Employee Acknowledgement

All employees are required to read, understand, and acknowledge this policy as a condition of their employment.

Signed by:

Susan Chishimba

Director, Corelink Consulting Ltd.

Date: 18th February 2025

Rowan J. Vos

Director, Corelink Consulting Ltd.

Date: 18th February 2025