BMD SECURITIES LIMITED

NETWORK SECURITY POLICY

Policy created by	Designated Officer
Policy reviewed by	Technology Committee
Policy reviewed on	31-12-2024
Policy Approved by	Board of Directors
Policy approved on	28-04-2025

Version – 1.0

Purpose

The purpose of this Network Security Policy is to establish guidelines and procedures to secure the network infrastructure, data, and communication systems of our Company. This policy aims to mitigate risks, protect sensitive information, and ensure the availability and reliability of network resources.

Scope

This policy applies to all employees, contractors, vendors, and any other individuals who have access to the stock brokerage firm's network infrastructure and systems.

Policy Guidelines

Access Control

- Access to the network and systems shall be granted based on job responsibilities.
- User accounts must be unique to individuals and tied to specific job roles.
- Access permissions will be reviewed regularly and adjusted as needed.

Authentication and Passwords

- Strong, unique passwords are required for all user accounts.
- Multi-factor authentication (MFA) is mandatory for accessing sensitive systems.
- Passwords must be changed at regular intervals.

Network Monitoring

- Network traffic will be monitored for abnormal patterns and potential security threats.
- Regular audits of network logs will be conducted to identify and respond to suspicious activities.

Firewall Configuration

- Firewalls must be configured to restrict unauthorized access and protect against external threats.
- Regular reviews of firewall rules and configurations will be conducted.

Data Encryption

- All sensitive data transmitted over the network must be encrypted using secure protocols.
- Virtual Private Network (VPN) connections are required for remote access.

Wireless Network Security

- Wireless networks must be secured with strong encryption and authentication mechanisms.

- Guest Wi-Fi networks should be isolated from the main network.

Incident Response Plan

- An incident response plan will be established to promptly address and mitigate security incidents.
- Employees shall be trained on reporting security incidents and breaches.

Remote Access Security

- Remote access to company networks must adhere to the same security standards as on-site access.
- Secure connections, such as VPNs, must be used for remote access.

Vendor Security

Third-party vendors with network access must comply with security standards and undergo periodic security assessments.

Compliance and Legal Considerations

Regulatory Compliance

The network security policy will adhere to relevant financial regulations and industry standards.

Audit and Assessment

Periodic audits and security assessments will be conducted to ensure compliance with this policy.

Employee Responsibilities

Employees are responsible for using the network resources in a secure and responsible manner. Any suspicious activity or potential security vulnerabilities must be reported promptly.

Change in the Policy will be adopted as and when required by the company and is binding on all the Staff/Employees/and Directors of the Company.

BMD Securities Limited

BMD SECURITIES LTD

Utpal Mallick

Utpal Mallick
CISO
Dated: - 30-04-2025