CYBER SECURITY POLICY

NWH Group Limited
Reviewed- January 2026

POLICY STATEMENT

At NWH Group, we recognise the critical importance of cybersecurity in safeguarding our information assets, ensuring the privacy and integrity of our data, and protecting our operations from potential threats. This Cyber Security People Policy outlines the responsibilities of all employees, contractors, and third parties in maintaining a secure and resilient cybersecurity environment.

PURPOSE

This policy establishes guidelines and expectations for individuals accessing NWH Group's information systems and data, promoting a culture of awareness, responsibility, and vigilance in the face of cyber threats.

POLICY SCOPE

This policy applies to all employees, contractors, and third parties accessing NWH Group's information systems, networks, and data.

POLICY GUIDELINES

1. **User Access Control 1.1. Account Management:**

Access to information systems will be granted based on job roles and responsibilities. User accounts must be promptly deactivated or modified when job roles change or when individuals leave the organisation.

I. **Password Security:**

Users must create strong passwords and refrain from sharing them with others.

Passwords must be changed regularly, and multi-factor authentication (MFA) will be enforced to access sensitive systems.

2. Data Protection

i. Data Classification:

Employees must adhere to the data classification policy, categorising information based on sensitivity and confidentiality.

ii. Data Handling:

Confidential information must be handled with care and shared only with authorised individuals. When transmitting sensitive data, encryption must be used.

3. Security Awareness

i. Training:

Regular cybersecurity awareness training sessions will be conducted for all employees. Employees are encouraged to report any suspicious activities or security incidents promptly.

ii. Reporting:

Employees must immediately report any security incidents, such as malware, phishing attempts, or unauthorised access, to the IT department.

4. Device Security

i. Endpoint Protection:

All devices connected to the NWH Group network must have up-to-date antivirus software and security patches.

ii. Portable Devices:

Portable devices containing company data must be encrypted, and their use for business purposes must comply with company policies.

5. Incident Response

i. Reporting Incidents:

Employees must promptly report any cybersecurity incidents to the IT department. An incident response plan will be activated to address and mitigate the impact of security breaches.

CYBER SECURITY POLICY

6. Compliance

i. **Regulatory Compliance**:

Employees must adhere to all applicable cybersecurity laws and regulations. Regular audits will be conducted to ensure compliance with cybersecurity policies.

Enforcement

Non-compliance with this Cyber Security People Policy may result in disciplinary action, including but not limited to warnings, suspension, termination, and legal action as appropriate.

REVIEW AND REVISION

This policy will be reviewed annually and updated as needed to address emerging cyber threats and changes in the business environment.

Signed: Date: 15/01/2025

Gavin Money

Gavin Money

Managing Director