IT Security & Acceptable Use Policy
Version: 2025-01
Company: NMT
Region: Global (EN)
Effective Date: 07 December 2025
Review Date: 07 December 2025

---

1. Purpose & Scope

The IT Security & Acceptable Use Policy defines the standards and requirements for the secure use of NMT's technology resources. Its purpose is to protect company data, systems, intellectual property, and user privacy while enabling employees and third-party users to carry out their responsibilities effectively.

This policy applies globally to:

- All employees, contractors, consultants, and interns
- Third-party users with access to company devices, networks, cloud services, or IT-managed tools
- All work environments including corporate offices, remote work locations, and client sites

1.1 Devices Covered

- Laptops and desktops issued by NMT
- Mobile devices including smartphones and tablets
- Employee-owned devices under the Bring Your Own Device (BYOD) program

1.2 Networks

- Company-owned wired and wireless networks
- Remote access networks via Virtual Private Network (VPN)
- Public Wi-Fi connections used to access company resources

1.3 Cloud Services

- Approved cloud applications such as Google Workspace and Microsoft 365
- Authorized third-party SaaS tools and integrated systems

---

2. User Responsibilities

2.1 Security Hygiene

- Install updates and patches for operating systems and applications promptly.
- Use strong, unique passwords for different accounts and systems.
- Follow all IT security guidelines and best practices.

Example:
Failure to update outdated software can expose devices to known vulnerabilities that cybercriminals exploit.

2.2 Reporting Incidents

- Immediately report any suspicious activity, unauthorized access, or security incidents to the IT department.

Example:
Notifying IT about unusual login attempts helped prevent unauthorized access in a previous case.

2.3 Training

- Complete mandatory annual cybersecurity and acceptable use training.
- Participate in refresher courses and simulations as required.

Manager Checklist:

- Confirm team completion of training.
- Schedule follow-ups for overdue or incomplete training.

---

3. Authentication

3.1 Password Rules

- Minimum length: 12 characters
- Must include uppercase, lowercase, numbers, and symbols
- Password changes required every 90 days

3.2 Multi-Factor Authentication (MFA)

- Mandatory for accessing all critical systems and administrative tools.

3.3 Single Sign-On (SSO)

- Required wherever available to streamline authentication securely.

3.4 Password Managers

- Use only NMT-approved password management tools.

Authentication Requirements for New Hires

Requirement	Description
Password Length	Minimum 12 characters
Password Change Frequency	Every 90 days
MFA	Required for critical systems
SSO	Use where available
Password Manager	Company-approved

---

4. Device Security

4.1 Laptops and Mobile Devices

- Full-disk encryption must be enabled.
- Screen lock must activate after a short period of inactivity.
- Only approved applications may be installed on company devices.

4.2 BYOD (Bring Your Own Device)

- Personal devices must meet security standards including updated software and enabled encryption.
- Non-compliant devices may not be used for company work.

Example:
A lost personal device without encryption may expose confidential data.

4.3 Patching and Updates

- Operating systems, browsers, and business applications must be updated regularly.

Manager Checklist:

- Confirm device encryption and compliance status.
- Ensure patching and update schedules are followed.

---

5. Network Security

5.1 VPN Usage

- Employees must use the company VPN for remote access to internal systems.

5.2 Public Wi-Fi Restrictions

- Avoid accessing sensitive data on public Wi-Fi unless using a VPN.

Example:
Checking email on unsecured networks increases risk of data interception.

5.3 Restricted Locations

- Access from geographic regions identified as high-risk is prohibited.

Manager Checklist:

- Reinforce VPN requirements.
- Review team compliance with location-based restrictions.

---

6. Data Handling

6.1 Classification Levels

- **Confidential:** High-sensitivity company data
- **Internal Use Only:** Non-public, operational data
- **Public:** Approved for public distribution

6.2 Storage and Sharing

- Store data only on approved platforms.
- Use secure methods (e.g., encrypted email, approved drives) to share sensitive data.

6.3 Retention

- Follow the retention schedule outlined in NMT's Data Retention Policy.

6.4 Data Loss Prevention (DLP)

- DLP tools may be used to prevent unauthorized data transfer or leakage.

Manager Checklist:

- Validate team understanding of data classifications.
- Monitor adherence to data storage and sharing requirements.

---

7. Cloud & SaaS Usage

7.1 Approved Apps

- Employees must use only company-approved cloud applications.

7.2 Shadow IT Risks

- Use of unauthorized applications is prohibited due to security and compliance risks.

7.3 API Keys

- API keys must be encrypted, stored securely, and rotated periodically.

Manager Checklist:

- Review employees' app usage for unauthorized tools.
- Educate teams on dangers associated with Shadow IT.

---

8. Email & Messaging

8.1 Phishing Awareness

- Employees must avoid clicking suspicious links, attachments, or sender addresses.

8.2 Auto-Forwarding Rules

- Auto-forwarding company emails to personal accounts is strictly prohibited.

Example:
Reporting a suspicious message prevents credential theft.

Manager Checklist:

- Conduct periodic phishing simulations.

- Reinforce email and messaging safety protocols.

---

9. Access Control

9.1 Least Privilege Principle

- Grant only the minimum access necessary for job duties.

9.2 Joiner–Mover–Leaver Process

- IT must be notified immediately of onboarding, role changes, and departures to adjust access rights.

9.3 Access Audits

- Regular audits must be conducted to verify appropriate access levels.

Manager Checklist:

- Review user access rights quarterly.
- Ensure timely updates through joiner-mover-leaver procedures.

---

10. Monitoring & Privacy Notice

10.1 What's Monitored

- Activity on company devices, networks, and cloud systems
- Email and messaging for compliance and threat detection

10.2 Why It's Monitored

- To protect company assets
- To maintain system integrity
- To ensure adherence to security policies

10.3 Retention

- Monitoring data is retained for 12 months unless required longer by legal obligations.

---

11. Incident Reporting

11.1 What to Report

- Unauthorized access attempts
- Data breaches
- Suspicious emails, messages, or activities

11.2 How to Report

- Use the designated security incident reporting system or contact the IT Security team.

11.3 Timelines

- Incidents must be reported within 24 hours of identification.

11.4 P1/P2 Triage Categories

- **P1:** Critical incidents requiring immediate escalation
- **P2:** High-risk but non-critical incidents

Manager Checklist:

- Ensure all team members know proper reporting steps.
- Review response procedures regularly.

---

12. Third-Party & Vendor Access

12.1 Due Diligence

- Conduct security risk assessments before granting vendor access.

12.2 NDAs

- All third parties must sign Non-Disclosure Agreements before receiving access.

12.3 Revocation

- Access must be revoked immediately when a vendor no longer requires system access.

Manager Checklist:

- Review vendor access periodically.
- Ensure all vendors maintain NDA compliance.

13. Disciplinary Actions for Violations

Violations of this policy may result in corrective measures, up to and including termination of employment.
Serious breaches may also lead to legal action, financial liabilities, or reporting to regulatory authorities.

---

14. Appendix

14.1 Glossary

- **BYOD:** Bring Your Own Device
- **DLP:** Data Loss Prevention
- **MFA:** Multi-Factor Authentication
- **SSO:** Single Sign-On

14.2 Manager Checklist

- Review and understand all policy requirements.
- Ensure direct reports adhere to acceptable use and security standards.

14.3 Related Policies

- Code of Conduct & Ethics Policy
- Remote Work Policy

This IT Security & Acceptable Use Policy reinforces NMT's commitment to protecting its information assets, supporting safe digital practices, and enabling secure collaboration across global teams.