1. IT Security & Acceptable Use Policy

Version: 2025-01
Company: NMT
Region: Global (EN)

---

2. Purpose & Scope

The IT Security & Acceptable Use Policy establishes guidelines for the secure use of company technology resources. It applies to all employees, contractors, and third-party users who access company devices, networks, cloud services, and third-party tools.

2.1 Devices Covered

- Laptops and desktops
- Mobile devices (smartphones, tablets)
- Personal devices under the BYOD policy

2.2 Networks

- Company-owned networks
- Remote access via VPN
- Public Wi-Fi connections

2.3 Cloud Services

- Approved cloud applications (e.g., Google Workspace, Microsoft 365)
- Third-party tools and services

---

3. User Responsibilities

3.1 Security Hygiene

- Regularly update software and applications.
- Use strong, unique passwords for different accounts.

Example:
Failure to update software may lead to vulnerabilities exploited by cybercriminals.

3.2 Reporting Incidents

- Report any suspicious activity or security incidents immediately to IT.

Example:
Unusual login attempts are reported to IT, preventing potential breaches.

3.3 Training

- Complete mandatory annual security training.

Manager Checklist:
- Ensure team completion of training.
- Schedule follow-up for missed deadlines.

---

4. Authentication

4.1 Password Rules

- Minimum 12 characters with uppercase, lowercase, numbers, and symbols.
- Change passwords every 90 days.

4.2 Multi-Factor Authentication (MFA)

- Required for all critical systems.

4.3 Single Sign-On (SSO)

- Use SSO where available.

4.4 Password Managers

- Use company-approved password managers.

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

---

5. Device Security

5.1 Laptops and Mobiles

- Enable encryption on all devices.
- Use screen locks to prevent unauthorized access.

5.2 BYOD

- Personal devices must meet company security standards.

Example:
Unencrypted personal devices pose data exposure risks if lost.

5.3 Patching

- Regularly update operating systems and applications.

Manager Checklist:
- Confirm device encryption.
- Ensure regular patching.

---

6. Network Security

6.1 VPN Usage

- Employees must use the company VPN for remote access.

6.2 Public Wi-Fi Restrictions

- Avoid accessing sensitive information over public networks.

Example:
Checking work email on public Wi-Fi risks intercepted communication.

6.3 Restricted Locations

- Access from high-risk locations is prohibited.

Manager Checklist:
- Reinforce VPN rules.
- Monitor compliance with Wi-Fi restrictions.

---

7. Data Handling

7.1 Classification Levels

- **Confidential:** Sensitive company data
- **Internal Use Only:** Non-public internal information
- **Public:** Information meant for public consumption

7.2 Storage and Sharing

- Store data only in approved locations.
- Use secure methods for sharing sensitive information.

7.3 Retention

- Follow retention rules outlined in the Data Retention Policy.

7.4 Data Loss Prevention (DLP)

- Implement DLP measures to protect sensitive data.

Manager Checklist:
- Ensure understanding of classification levels.
- Monitor adherence to storage rules.

---

8. Cloud & SaaS Usage

8.1 Approved Apps

- Use only company-approved cloud applications.

8.2 Shadow IT Risks

- Avoid unauthorized applications that pose security risks.

8.3 API Keys

- Securely store and manage API keys.

Manager Checklist:
- Review app usage.
- Educate about shadow IT dangers.

---

9. Email & Messaging

9.1 Phishing Awareness

- Do not click unknown links or attachments.

9.2 Auto-Forwarding Rules

- Auto-forwarding to personal accounts is prohibited.

Example:
Reporting a suspicious email prevents credential theft.

Manager Checklist:
- Conduct phishing simulations.
- Reinforce email security rules.

---

10. Access Control

10.1 Least Privilege Principle

- Grant access only as required for job duties.

10.2 Joiner-Mover-Leaver Process

- Follow protocols for onboarding, role changes, and offboarding.

10.3 Audits

- Conduct regular access-rights audits.

Manager Checklist:
- Review access rights quarterly.
- Ensure compliance with joiner-mover-leaver procedures.

---

11. Monitoring & Privacy Notice

11.1 What's Monitored

- User activity on company devices and networks
- Email and messaging for compliance

11.2 Why It's Monitored

- To protect company assets and ensure compliance

11.3 Retention

- Monitoring data retained for 12 months

---

12. Incident Reporting

12.1 What to Report

- Unauthorized access
- Data breaches
- Suspicious activity

12.2 How to Report

- Use the designated reporting system.

12.3 Timelines

- Report incidents within 24 hours.

12.4 P1/P2 Triage

- Classify incidents based on severity.

Manager Checklist:

- Ensure awareness of reporting steps.
- Review response procedures.

---

13. Third-Party & Vendor Access

13.1 Due Diligence

- Conduct risk assessments before granting access.

13.2 NDAs

- Require all third parties to sign NDAs.

13.3 Revocation

- Revoke access immediately when no longer needed.

Manager Checklist:

- Review access quarterly.
- Ensure NDA compliance.

---

14. Disciplinary Actions for Violations

Violations of this policy may result in disciplinary action, up to and including termination.

---

15. Appendix

15.1 Glossary

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

15.2 Manager Checklist

- Review and understand policy requirements.
- Ensure team compliance.

15.3 Related Policies

- Code of Conduct
- Remote Work Policy

15.4 FAQ

Q1: What if I forget my password?
A1: Use the reset feature or contact IT.

Q2: Can I use personal devices for work?
A2: Yes, following BYOD requirements.

Q3: What counts as a security incident?
A3: Any unauthorized access or suspected breach.

Q4: How often should passwords be changed?
A4: Every 90 days.

Q5: What if I receive a suspicious email?
A5: Report it immediately; do not click links.

Q6: Can I use unapproved cloud services?
A6: No, unauthorized applications are prohibited.

Q7: Is employee activity monitored?
A7: Yes, for compliance and security purposes.
