nordomatic®
Change today. Impact tomorrow.

The Nordomatic Policy
Cyber Security
2025

Document Classification:	**Internal**
Dated:	01.01.2025
Document Author:	Group IT Director
Document Owner:	CEO Toke Juul

About the Policy

This policy protects Nordomatic data, systems, and resources from cyber threats, including unauthorized access, data breaches, and data loss. All employees and contractors must follow this policy to maintain the security and confidentiality of organizational assets.

This policy applies to all employees, contractors, and third-party users accessing Nordomatic systems, networks, or data.

Security Guidelines

Access Control

- Only authorized personnel may access systems and data.
- Access should be limited to only the resources needed to perform job functions.
- Use unique, strong passwords (at least 8 characters, including letters, numbers, and symbols) and change them every 365 days.
- Multi-factor authentication (MFA) must be enabled on all available accounts.

Data Protection

- Sensitive data must be encrypted in storage and during transmission.
- Do not store sensitive information on unauthorized devices.
- Follow data retention guidelines and securely dispose of data when no longer needed.

Device Security

- All devices must have updated antivirus software and regular security updates must be monitored by Microsoft Intune.
- Personal devices used for work must follow the same security standards as organization-issued devices.
- Report lost or stolen devices immediately to the IT department, which is managed with security implications of remote wipe and disabling accounts.

Network Security

- Connect to Nordomatic network and infrastructure only through approved secure connections, such as a VPN Client.
- Avoid connecting to public or unsecured Wi-Fi networks while accessing sensitive information. When you cannot access a secure network, share the internet through your mobile device.
- Network monitoring and firewall protection are in place and cannot be tampered with without authorization.

Email and Communication

- Do not open suspicious emails, links, or attachments from unknown senders.
- Use Nordomatic official email for all work-related communication.
- Report phishing attempts or suspicious emails to the Service Portal.

Incident Reporting

- Report any security incidents, breaches, or suspected vulnerabilities immediately to the Service Portal.
- Employees must cooperate fully with incident response and investigation efforts.
- Violation of this policy may lead to disciplinary actions, up to and including termination.

Review and Update

This policy may be reviewed and updated to address emerging security threats. All employees, suppliers, and partners are expected to understand and contribute to upholding the principles outlined in this policy.

How to contact us

Please contact your direct manager or your local IT department with any questions regarding this policy.