Service Description — Managed IT Services

Scope, inclusions and exclusions of Nord Node's managed service modules

Version 1.0 · Effective: 24 September 2026

This document forms part of the Agreement between Nord Node AB and the Customer. It applies where an Order Form has been signed and does not apply to use of Nord Node's website.

1. Purpose

1.1 This Service Description sets out what is included in Nord Node's Managed Services. It forms part of the Agreement with each Customer that orders Managed Services. Terms defined in the General Terms of Service have the same meaning here.

1.2 The Order Form states which service modules the Customer has ordered and the quantities covered. Only the modules stated in the Order Form are included.

2. Platforms used to deliver the Services

2.1 Nord Node delivers the Services using the following platforms, which Nord Node licenses and operates:

Platform	Used for
Tanium Endpoint Management (and Tanium Threat Response where ordered)	Endpoint inventory, patching, software deployment, configuration management, endpoint visibility and remediation
ServiceNow (IT and customer service management)	Customer portal, ticketing, incidents, service requests, service level tracking, knowledge base and configuration management database (CMDB)
Keeper MSP and KeeperPAM	Secure storage of credentials used to administer the Customer Environment, and control of privileged administrative access
Microsoft 365, Microsoft Entra ID, Microsoft Intune, Microsoft Defender and Microsoft Quick Assist	Nord Node's own working environment, administration of the Customer Environment, and remote support

2.2 These platforms are licensed to Nord Node, not to the Customer. The Customer receives access to the ServiceNow customer portal for the duration of the Services, and management agents are installed on covered devices. The Customer receives no separate licence to the platforms themselves, and access ends when the Services end (General Terms section 18.2).

2.3 Where these platforms process personal data on the Customer's behalf, the providers act as Nord Node's sub-processors. They are listed in the Data Processing Agreement and the Sub-processor List, and changes follow the notice procedure in that agreement.

2.4 Products licensed by the Customer in its own Microsoft tenant, such as Microsoft 365, Entra ID, Defender and Intune, remain the Customer's own services under the Customer's agreement with Microsoft. Nord Node administers them on the Customer's behalf.

3. Customer licence prerequisites

3.1 Several modules depend on licences held by the Customer. The Order Form states which licences are required for the modules ordered. Typical requirements are:

Module	Customer licences normally required
Identity and access management	Microsoft Entra ID P1; Entra ID P2 for Privileged Identity Management and identity risk policies
Endpoint security	Microsoft Defender for Business, or Defender for Endpoint P2 for advanced detection and response
Email and collaboration security	Microsoft Defender for Office 365 P1; P2 for Threat Explorer and advanced investigation
Device management through Intune	Microsoft Intune
Identity threat protection, cloud application security, XDR	Microsoft Defender for Identity, Defender for Cloud Apps, Defender XDR
Data governance	Microsoft Purview
Security information and event management	Microsoft Sentinel, with Azure consumption charged as described in the Order Form

3.2 If the Customer does not hold the required licence, the affected part of the module cannot be delivered. Nord Node will inform the Customer and may propose an alternative (General Terms section 6.1(d)).

4. Onboarding

4.1 At the start of the Managed Services, Nord Node will:

- review the Customer Environment covered by the Services and document the starting position in the CMDB;
- create the Customer's account and Users in the ServiceNow customer portal;
- deploy the Tanium agent to covered devices and, where Intune is used, enrol those devices;
- enable the security features included in the Customer's Microsoft licences, in line with Nord Node's security baseline;
- store the credentials needed to administer the Customer Environment in Keeper, separated per Customer;
- set up named administrator accounts for Nord Node personnel, protected by multi-factor authentication;
- agree Authorised Contacts, escalation contacts and the security contact;
- identify systems, devices and software that do not meet the minimum requirements in section 13, and record them as exceptions; and
- provide an onboarding report with recommendations.

4.2 Onboarding is charged as a one-off fee if stated in the Order Form. Remediation of issues found during onboarding is charged as Professional Services unless included in the Order Form.

5. Service desk and customer portal

5.1 Includes:

- access to the ServiceNow customer portal for Authorised Contacts and Users, for creating and tracking tickets, submitting service requests, following service level status and reading knowledge articles;

- service desk support for Users by the portal, e-mail and telephone during support hours, in accordance with the SLA;
- remote support for covered devices using Microsoft Quick Assist or another remote support tool agreed with the Customer. A remote session can only be started when the User accepts it, and the User can end it at any time;
- User onboarding and offboarding: creating, changing and disabling accounts, licences, group memberships and mailboxes, on request from an Authorised Contact;
- password resets and multi-factor authentication resets, after verifying the requester's identity; and
- advice on the day-to-day use of standard office software.

5.2 Offboarding requests are processed within the response times in the SLA. For urgent offboarding, such as the immediate removal of a User's access, the Authorised Contact should contact Nord Node by telephone and the request will be treated as Priority 1.

5.3 Portal accounts are personal. The Customer is responsible for telling Nord Node when a portal User should be removed.

6. Managed Device

6.1 Includes, for covered Windows and macOS computers and, where stated in the Order Form, mobile devices:

- deployment and operation of the Tanium agent, giving hardware and software inventory, configuration management and endpoint visibility;
- operating system patching: security updates are deployed within 14 days of release for critical and high-severity updates, and within 30 days for other updates, subject to testing and exceptions agreed with the Customer;
- third-party application patching for applications in Nord Node's supported catalogue;
- software deployment and, where enabled, self-service software installation for Users;
- monitoring of device health, patch status and configuration drift, reviewed on each Business Day, with remediation of deviations;
- device compliance policies, disk encryption and screen-lock enforcement; and
- remote wipe or lock of lost or stolen devices on request from an Authorised Contact, where the device is managed by Intune or another platform that supports it.

6.2 Mobile device management, Windows Autopilot provisioning and mobile application management are delivered through Microsoft Intune where the Customer holds Intune licences and the module is stated in the Order Form.

6.3 Hardware repair, warranty handling with the manufacturer, and replacement devices are not included unless stated in the Order Form. Nord Node will assist with warranty cases at its hourly rates.

7. Identity and access management

7.1 Includes:

- administration of the Customer's Microsoft 365 tenant within the scope of standard settings: users, groups, licences, shared mailboxes, SharePoint and Teams permissions;
- management of Microsoft Entra ID conditional access, multi-factor authentication and single sign-on policies in line with Nord Node's security baseline;
- device-based access policies, where the Customer's licences support them;
- identity risk policies and Privileged Identity Management, where the Customer holds Entra ID P2;
- monitoring of Microsoft service health and communication of relevant incidents; and
- a quarterly review of administrator roles and guest access, where stated in the Order Form.

7.2 The Customer remains the owner of its tenant and retains at least one administrator account under its own control (General Terms section 10.3).

8. Endpoint and email security

8.1 **Endpoint security.** Deployment and management of Microsoft Defender for Business or Defender for Endpoint: antivirus, behavioural detection, endpoint detection and response, automated investigation, device isolation and remediation, together with security baseline configuration.

8.2 **Email and collaboration security.** Management of Microsoft Defender for Office 365: anti-phishing, anti-malware, Safe Links and Safe Attachments, and, where the Customer holds P2, Threat Explorer and advanced automated investigation and response.

8.3 **Alert handling.** Security alerts are reviewed during support hours. Confirmed threats on covered devices are investigated and contained, for example by isolating a device or removing malicious files.

8.4 **Outside support hours.** Nord Node does not monitor alerts outside support hours and does not operate a security operations centre, unless a managed detection and response (MDR) service is stated in the Order Form (section 11.6).

8.5 **Beyond containment.** Incident response beyond initial containment on covered devices, such as forensic investigation, restoring large parts of the environment or handling contacts with authorities, is charged as Professional Services (General Terms section 7.5).

9. Credential and privileged access management

9.1 Credentials used by Nord Node to administer the Customer Environment are stored in Keeper, with vaults separated per Customer and access limited to the personnel who need them. Keeper's architecture is designed so that vault contents are encrypted on the device and are not readable by the provider.

9.2 Where KeeperPAM is stated in the Order Form, privileged administrative access is brokered through it, with controlled technician sessions and credential isolation.

9.3 On request, Nord Node will hand over credentials to the Customer, and will do so as part of exit assistance (General Terms section 15.1(a)).

10. Backup

10.1 Backup is included only where an Order Form states it. The Order Form states the platform, the systems and data covered, the backup frequency, the retention period and the recovery objectives.

10.2 Nord Node offers backup on the following platforms. The platform selected for the Customer is stated in the Order Form:

Platform	Typically used for
Veeam	Microsoft 365, physical servers, virtual machines and endpoints, including image-based backup and bare-metal recovery
Veeam Backup for Microsoft 365	Exchange Online, SharePoint, OneDrive and Teams data, with separate retention policies
Microsoft 365 Backup	Exchange Online, SharePoint Online and OneDrive, using Microsoft's native backup service
Rubrik, including Rubrik Microsoft 365 Protection	Enterprise environments requiring immutable, cyber-resilience-focused recovery
Veeam Agent	Full-machine backup of selected critical laptops and workstations

10.3 The retention, recycle-bin, versioning and hold features built into Microsoft 365 are not a backup service, and Nord Node does not present them as one. They do not protect against all forms of data loss, such as deletion discovered after the retention period has expired.

10.4 Where backup is ordered, Nord Node will monitor backup jobs on each Business Day, act on failures, and carry out restore tests at the frequency stated in the Order Form, recording the result. Unless the Order Form states otherwise, backup data is stored within the EU/EEA and a restore test is carried out at least once per quarter. Nord Node does not guarantee that every item of data can be restored, but will use its best reasonable efforts to restore data from the most recent available backup.

10.5 Data outside the scope stated in the Order Form is not backed up. Where no backup module is ordered, the Customer is responsible for protecting its data against loss (General Terms section 6.2), and Nord Node will on request explain the options and quote for them.

10.6 When the backup service ends, backup data is kept for 30 days to allow export and is then deleted (General Terms section 15.3 and Data Processing Agreement section 14).

11. Optional and advanced modules

11.1 **Tanium Threat Response.** Deep endpoint visibility and response: threat hunting, endpoint telemetry, process and network visibility, investigation, isolation and remediation.

11.2 **Microsoft Defender for Identity.** Detection of identity-based attacks, including credential attacks, suspicious authentication activity, lateral movement and identity reconnaissance.

11.3 **Microsoft Defender for Cloud Apps.** Monitoring of SaaS and cloud application risk, including shadow IT discovery, suspicious activity and session controls.

11.4 **Microsoft Defender XDR.** Correlation of security signals across endpoint, e-mail, identity and cloud applications, with investigation, hunting and automated response.

11.5 **Microsoft Sentinel.** Central security log collection, analytics rules, automation and long-term investigation. Azure consumption for Sentinel is charged as a usage-based Third-Party Service (General Terms section 12.1(c)).

11.6 **Managed detection and response (MDR).** Monitoring and response outside Nord Node's support hours is delivered by a specialist provider. This module is available only where the Order Form names the provider. The provider is added to the Sub-processor List before the service starts, with the notice period in the Data Processing Agreement.

11.7 **Microsoft Purview.** Data loss prevention, sensitivity labels, retention and information protection policies.

11.8 **Network security.** Firewall, secure internet access, VPN or zero-trust network access and network segmentation are delivered using the Customer's own network platform. The platform, scope and responsibilities are stated in the Order Form.

12. Documentation, CMDB and reporting

12.1 Nord Node maintains documentation of the Customer Environment covered by the Services, including tenant information, configurations and operating procedures, in ServiceNow and in Nord Node's Microsoft 365 environment.

12.2 Assets and their relationship to Customers and services are recorded in the ServiceNow CMDB, populated from Tanium where the integration is enabled.

12.3 Nord Node provides a service report at the frequency stated in the Order Form, and at least quarterly, covering tickets, patch status, security status and recommendations. Nord Node and the Customer will hold a service review at least once a year.

12.4 Documentation of the Customer Environment is handed over as part of exit assistance (General Terms section 15.1(b)).

13. Minimum requirements

13.1 To be covered by the Managed Services, devices and systems must:

- run an operating system version that is supported by its manufacturer with security updates, and that is supported by the Tanium agent;
- have a valid licence for all software;
- be covered by the Customer licences listed in section 3 for the modules ordered; and
- have an internet connection that allows the management agents to communicate with Nord Node's platforms.

13.2 Devices or systems that do not meet these requirements are recorded as exceptions and supported on a reasonable-efforts basis only (General Terms section 7.3).

14. Exclusions

14.1 Unless stated in the Order Form, the Managed Services do not include:

- project work, migrations, new installations, network redesign or the introduction of new systems;
- support for business applications not listed in the Order Form, such as ERP, accounting or industry-specific software, beyond basic troubleshooting and contact with the software vendor;
- support for private devices, except enrolment in the Customer's management platform where agreed;
- on-site work, which is charged by the hour plus travel;
- training beyond short guidance in connection with support requests;
- monitoring or response outside support hours, unless MDR is ordered under section 11.6;
- work caused by the Customer's breach of the Agreement or the Acceptable Use Policy, or by changes made by the Customer or third parties without Nord Node's involvement; and
- work on systems recorded as exceptions under section 13.

14.2 Excluded work may be ordered as Professional Services at the rates in the Order Form.

Related documents

Document	Web address
General Terms of Service	https://www.nordnode.se/en/dam/nordnode/legal/final/document/nordnode-general-terms-en.pdf
Data Processing Agreement	https://www.nordnode.se/en/dam/nordnode/legal/final/document/nordnode-data-processing-agreement-en.pdf
Sub-processor List	https://www.nordnode.se/en/dam/nordnode/legal/final/document/nordnode-subprocessors-en.pdf
SLA and Support Policy	https://www.nordnode.se/en/dam/nordnode/legal/final/document/nordnode-sla-en.pdf