Tjänstebeskrivning — Förvaltade IT-tjänster

Omfattning, vad som ingår och vad som inte ingår i Nord Nodes tjänstemoduler

Version 1.0 · Gäller från: 24 september 2026

> Detta dokument utgör en del av Avtalet mellan Nord Node AB och Kunden. Det gäller när en Beställning har undertecknats och gäller inte för användning av Nord Nodes webbplats.

1. Syfte

1.1 Denna Tjänstebeskrivning anger vad som ingår i Nord Nodes Förvaltade tjänster. Den utgör en del av Avtalet med varje Kund som beställer Förvaltade tjänster. Begrepp som definieras i Allmänna villkor har samma betydelse här.

1.2 Beställningen anger vilka tjänstemoduler Kunden har beställt och vilka antal som omfattas. Endast de moduler som anges i Beställningen ingår.

2. Plattformar som används för att leverera Tjänsterna

2.1 Nord Node levererar Tjänsterna med följande plattformar, som Nord Node licensierar och driver:

Plattform	Används för
Tanium Endpoint Management (och Tanium Threat Response när det har beställts)	Inventering av enheter, uppdateringar, programdistribution, konfigurationshantering, synlighet och åtgärder på slutpunkter
ServiceNow (IT- och kundserviceplattform)	Kundportal, ärendehantering, incidenter, beställningar, uppföljning av servicenivåer, kunskapsbank och CMDB
Keeper MSP och KeeperPAM	Säker lagring av de inloggningsuppgifter som används för att administrera Kundens miljö, samt kontroll av privilegierad administrativ åtkomst
Microsoft 365, Microsoft Entra ID, Microsoft Intune, Microsoft Defender och Microsoft Quick Assist	Nord Nodes egen arbetsmiljö, administration av Kundens miljö och fjärrsupport

2.2 Plattformarna är licensierade till Nord Node, inte till Kunden. Kunden får tillgång till ServiceNow-kundportalen under Tjänsternas löptid, och förvaltningsagenter installeras på de enheter som omfattas. Kunden får ingen separat licens till plattformarna och åtkomsten upphör när Tjänsterna upphör (punkt 18.2 i Allmänna villkor).

2.3 När plattformarna behandlar personuppgifter för Kundens räkning är leverantörerna Nord Nodes underbiträden. De anges i Personuppgiftsbiträdesavtalet och i förteckningen över underbiträden, och ändringar följer underrättelseförfarandet i det avtalet.

2.4 Produkter som Kunden licensierar i sin egen Microsoft-miljö, såsom Microsoft 365, Entra ID, Defender och Intune, förblir Kundens egna tjänster enligt Kundens avtal med Microsoft. Nord Node administrerar dem för Kundens räkning.

3. Licenser som Kunden måste ha

3.1 Flera moduler förutsätter licenser som Kunden innehar. Beställningen anger vilka licenser som krävs för de beställda modulerna. Normalt krävs:

Modul	Licenser som Kunden normalt behöver
Identitets- och åtkomsthantering	Microsoft Entra ID P1; Entra ID P2 för Privileged Identity Management och riskbaserade identitetspolicyer
Slutpunktsskydd	Microsoft Defender for Business, eller Defender for Endpoint P2 för avancerad detektion och respons
Skydd för e-post och samarbete	Microsoft Defender for Office 365 P1; P2 för Threat Explorer och avancerad utredning
Enhetshantering via Intune	Microsoft Intune
Identitetsskydd, molnappsäkerhet, XDR	Microsoft Defender for Identity, Defender for Cloud Apps, Defender XDR
Informationsstyrning	Microsoft Purview
Säkerhetsloggning och korrelation (SIEM)	Microsoft Sentinel, där Azure-förbrukning debiteras enligt Beställningen

3.2 Om Kunden inte har den licens som krävs kan den berörda delen av modulen inte levereras. Nord Node informerar Kunden och kan föreslå ett alternativ (punkt 6.1 (d) i Allmänna villkor).

4. Uppstart

4.1 Vid uppstarten av de Förvaltade tjänsterna ska Nord Node:

- gå igenom den del av Kundens miljö som omfattas av Tjänsterna och dokumentera utgångsläget i CMDB;
- skapa Kundens konto och Användare i ServiceNow-kundportalen;
- distribuera Tanium-agenten till de enheter som omfattas och, när Intune används, registrera enheterna där;
- aktivera de säkerhetsfunktioner som ingår i Kundens Microsoft-licenser, i enlighet med Nord Nodes säkerhetsbaslinje;
- lagra de inloggningsuppgifter som behövs för att administrera Kundens miljö i Keeper, åtskilda per Kund;
- skapa namngivna administratörskonton för Nord Nodes personal, skyddade med flerfaktorsautentisering;
- komma överens med Kunden om Behöriga kontaktpersoner, eskaleringskontakter och säkerhetskontakt;
- identifiera system, enheter och programvara som inte uppfyller minimikraven i punkt 13 och dokumentera dem som undantag; och
- lämna en uppstartsrapport med rekommendationer.

4.2 Uppstart debiteras som en engångsavgift om detta anges i Beställningen. Åtgärder av brister som upptäcks vid uppstarten debiteras som Konsulttjänster om de inte ingår enligt Beställningen.

5. Servicedesk och kundportal

5.1 Omfattar:

- tillgång till ServiceNow-kundportalen för Behöriga kontaktpersoner och Användare, för att skapa och följa ärenden, göra beställningar, följa servicenivåer och läsa kunskapsartiklar;
- servicedesk för Användare via portalen, e-post och telefon under supporttid, enligt SLA;
- fjärrsupport för enheter som omfattas, med Microsoft Quick Assist eller ett annat verktyg för fjärrsupport som avtalats med Kunden. En fjärrsession kan endast startas när Användaren accepterar den, och Användaren kan avsluta den när som helst;

- in- och utflyttning av Användare: skapa, ändra och inaktivera konton, licenser, gruppmedlemskap och brevlådor på begäran av en Behörig kontaktperson;
- återställning av lösenord och flerfaktorsautentisering, efter kontroll av den begärande personens identitet; och
- råd om den dagliga användningen av vanliga kontorsprogram.

5.2 Begäran om utflyttning hanteras inom de svarstider som anges i SLA. Vid brådskande utflyttning, till exempel när en Användares åtkomst omedelbart måste tas bort, ska den Behöriga kontaktpersonen kontakta Nord Node per telefon, och ärendet hanteras då som Prioritet 1.

5.3 Portalkonton är personliga. Kunden ansvarar för att meddela Nord Node när en portalanvändare ska tas bort.

6. Förvaltad enhet

6.1 Omfattar, för Windows- och macOS-datorer som omfattas och, om det anges i Beställningen, mobila enheter:

- installation och drift av Tanium-agenten, vilket ger inventering av hårdvara och programvara, konfigurationshantering och synlighet över slutpunkter;
- uppdatering av operativsystem: säkerhetsuppdateringar installeras inom 14 dagar från publicering för kritiska uppdateringar och uppdateringar med hög allvarlighetsgrad, och inom 30 dagar för övriga uppdateringar, med förbehåll för tester och undantag som avtalats med Kunden;
- uppdatering av tredjepartsprogram som ingår i Nord Nodes katalog över programvara som stöds;
- programdistribution och, där funktionen är aktiverad, självbetjäning för Användare vid programinstallation;
- uppföljning av enheternas status, uppdateringsnivå och konfigurationsavvikelser, som granskas varje Arbetsdag, med åtgärd av avvikelser;
- efterlevnadsregler för enheter, diskkryptering och krav på skärmlås; och
- fjärradering eller låsning av borttappade eller stulna enheter på begäran av en Behörig kontaktperson, när enheten hanteras av Intune eller en annan plattform som stöder det.

6.2 Hantering av mobila enheter, etablering med Windows Autopilot och hantering av mobilapplikationer levereras via Microsoft Intune när Kunden har Intune-licenser och modulen anges i Beställningen.

6.3 Reparation av hårdvara, garantiärenden hos tillverkaren och ersättningsenheter ingår inte om det inte anges i Beställningen. Nord Node bistår med garantiärenden mot timersättning.

7. Identitets- och åtkomsthantering

7.1 Omfattar:

- administration av Kundens Microsoft 365-miljö inom ramen för standardinställningar: användare, grupper, licenser, delade brevlådor samt behörigheter i SharePoint och Teams;
- förvaltning av villkorad åtkomst, flerfaktorsautentisering och enkel inloggning i Microsoft Entra ID i enlighet med Nord Nodes säkerhetsbaslinje;
- enhetsbaserade åtkomstregler, när Kundens licenser stöder dem;
- riskbaserade identitetspolicyer och Privileged Identity Management, när Kunden har Entra ID P2;
- bevakning av Microsofts driftstatus och information om relevanta störningar; och
- en kvartalsvis genomgång av administratörsroller och gäståtkomst, om det anges i Beställningen.

7.2 Kunden är fortsatt ägare till sin miljö och behåller minst ett administratörskonto under egen kontroll (punkt 10.3 i Allmänna villkor).

8. Skydd för slutpunkter och e-post

8.1 **Slutpunktsskydd.** Installation och förvaltning av Microsoft Defender for Business eller Defender for Endpoint: antivirus, beteendebaserad detektion, detektion och respons på slutpunkter, automatiserad utredning, isolering av enheter och åtgärder, samt konfiguration enligt säkerhetsbaslinje.

8.2 **Skydd för e-post och samarbete.** Förvaltning av Microsoft Defender for Office 365: skydd mot nätfiske och skadlig kod, Safe Links och Safe Attachments samt, när Kunden har P2, Threat Explorer och avancerad automatiserad utredning och respons.

8.3 **Hantering av larm.** Säkerhetslarm granskas under supporttid. Bekräftade hot på enheter som omfattas utreds och begränsas, till exempel genom att en enhet isoleras eller skadliga filer tas bort.

8.4 **Utanför supporttid.** Nord Node bevakar inte larm utanför supporttid och driver inget säkerhetscenter (SOC), om inte en tjänst för hanterad detektion och respons (MDR) anges i Beställningen (punkt 11.6).

8.5 **Utöver begränsning.** Incidenthantering som går utöver den initiala begränsningen på enheter som omfattas, såsom forensisk utredning, återställning av större delar av miljön eller kontakter med myndigheter, debiteras som Konsulttjänster (punkt 7.5 i Allmänna villkor).

9. Hantering av inloggningsuppgifter och privilegierad åtkomst

9.1 De inloggningsuppgifter som Nord Node använder för att administrera Kundens miljö lagras i Keeper, med valv åtskilda per Kund och åtkomst begränsad till den personal som behöver dem. Keepers arkitektur är utformad så att innehållet i valven krypteras på enheten och inte kan läsas av leverantören.

9.2 När KeeperPAM anges i Beställningen förmedlas privilegierad administrativ åtkomst genom den lösningen, med kontrollerade teknikersessioner och isolering av inloggningsuppgifter.

9.3 På begäran lämnar Nord Node över inloggningsuppgifter till Kunden, och gör det som en del av avvecklingsbiståndet (punkt 15.1 (a) i Allmänna villkor).

10. Säkerhetskopiering

10.1 Säkerhetskopiering ingår endast när en Beställning anger det. Beställningen anger plattform, vilka system och vilken data som omfattas, frekvens, lagringstid och återställningsmål.

10.2 Nord Node erbjuder säkerhetskopiering på följande plattformar. Vald plattform anges i Beställningen:

Plattform	Används normalt för
Veeam	Microsoft 365, fysiska servrar, virtuella maskiner och slutpunkter, inklusive avbildningsbaserad säkerhetskopiering och bare-metal-återställning
Veeam Backup for Microsoft 365	Exchange Online, SharePoint, OneDrive och Teams-data, med separata lagringsregler
Microsoft 365 Backup	Exchange Online, SharePoint Online och OneDrive, med Microsofts inbyggda tjänst
Rubrik, inklusive Rubrik Microsoft 365 Protection	Större miljöer som kräver oföränderliga säkerhetskopior och cyberåterställning
Veeam Agent	Fullständig säkerhetskopiering av utvalda kritiska bärbara datorer och arbetsstationer

10.3 De funktioner för kvarhållning, papperskorg, versionshantering och bevarandepolicy som är inbyggda i Microsoft 365 utgör inte en tjänst för säkerhetskopiering, och Nord Node beskriver dem inte som en sådan. De skyddar inte mot alla former av dataförlust, till exempel radering som upptäcks efter kvarhållningstidens utgång.

10.4 När säkerhetskopiering har beställts övervakar Nord Node säkerhetskopieringsjobben varje Arbetsdag, åtgärdar fel och genomför återställningstester med den frekvens som anges i Beställningen och dokumenterar resultatet. Om inte annat anges i Beställningen lagras säkerhetskopior inom EU/EES och ett återställningstest genomförs minst en gång per kvartal. Nord Node garanterar inte att all data kan återställas, men ska i skälig omfattning göra sitt bästa för att återställa data från den senast tillgängliga säkerhetskopian.

10.5 Data utanför den omfattning som anges i Beställningen säkerhetskopieras inte. Om ingen modul för säkerhetskopiering har beställts ansvarar Kunden för att skydda sin data mot förlust (punkt 6.2 i Allmänna villkor), och Nord Node redogör på begäran för alternativen och lämnar offert.

10.6 När tjänsten för säkerhetskopiering upphör sparas säkerhetskopiorna i 30 dagar för att möjliggöra export och raderas därefter (punkt 15.3 i Allmänna villkor och punkt 14 i Personuppgiftsbiträdesavtalet).

11. Valfria och avancerade moduler

11.1 **Tanium Threat Response.** Fördjupad synlighet och respons på slutpunkter: hotjakt, telemetri, insyn i processer och nätverkstrafik, utredning, isolering och åtgärder.

11.2 **Microsoft Defender for Identity.** Detektion av identitetsbaserade angrepp, såsom angrepp mot inloggningsuppgifter, misstänkt autentiseringsaktivitet, lateral förflyttning och kartläggning av identiteter.

11.3 **Microsoft Defender for Cloud Apps.** Bevakning av risker i SaaS- och molnapplikationer, inklusive upptäckt av skugg-IT, misstänkt aktivitet och sessionskontroller.

11.4 **Microsoft Defender XDR.** Korrelering av säkerhetssignaler från slutpunkter, e-post, identiteter och molnapplikationer, med utredning, hotjakt och automatiserad respons.

11.5 **Microsoft Sentinel.** Central insamling av säkerhetsloggar, analysregler, automatisering och långsiktig utredning. Azure-förbrukning för Sentinel debiteras som en förbrukningsbaserad Tredjepartstjänst (punkt 12.1 (c) i Allmänna villkor).

11.6 **Hanterad detektion och respons (MDR).** Bevakning och respons utanför Nord Nodes supporttid levereras av en specialiserad leverantör. Modulen är tillgänglig endast när Beställningen anger leverantören. Leverantören läggs till i förteckningen över underbiträden innan tjänsten startar, med den underrättelsetid som anges i Personuppgiftsbiträdesavtalet.

11.7 **Microsoft Purview.** Skydd mot dataförlust, känslighetsetiketter, kvarhållningsregler och informationsskydd.

11.8 **Nätverkssäkerhet.** Brandvägg, säker internetåtkomst, VPN eller ZTNA och nätverkssegmentering levereras med Kundens egen nätverksplattform. Plattform, omfattning och ansvarsfördelning anges i Beställningen.

12. Dokumentation, CMDB och rapportering

12.1 Nord Node upprätthåller dokumentation över den del av Kundens miljö som omfattas av Tjänsterna, inklusive uppgifter om molnmiljöer, konfigurationer och arbetsrutiner, i ServiceNow och i Nord Nodes Microsoft 365-miljö.

12.2 Tillgångar och deras koppling till kunder och tjänster registreras i ServiceNow CMDB, som fylls på från Tanium när integrationen är aktiverad.

12.3 Nord Node lämnar en tjänsterapport med den frekvens som anges i Beställningen, och minst kvartalsvis, som omfattar ärenden, uppdateringsstatus, säkerhetsstatus och rekommendationer. Nord Node och Kunden håller ett uppföljningsmöte minst en gång per år.

12.4 Dokumentationen över Kundens miljö lämnas över som en del av avvecklingsbiståndet (punkt 15.1 (b) i Allmänna villkor).

13. Minimikrav

13.1 För att omfattas av de Förvaltade tjänsterna ska enheter och system:

- ha en version av operativsystemet som får säkerhetsuppdateringar från tillverkaren och som stöds av Tanium-agenten;
- ha giltig licens för all programvara;
- omfattas av de kundlicenser som anges i punkt 3 för de beställda modulerna; och
- ha en internetanslutning som gör det möjligt för förvaltningsagenterna att kommunicera med Nord Nodes plattformar.

13.2 Enheter och system som inte uppfyller dessa krav dokumenteras som undantag och får support endast i skälig omfattning (punkt 7.3 i Allmänna villkor).

14. Undantag

14.1 Om inte annat anges i Beställningen omfattar de Förvaltade tjänsterna inte:

- projektarbete, migreringar, nyinstallationer, omdesign av nätverk eller införande av nya system;
- support för verksamhetssystem som inte anges i Beställningen, såsom affärssystem, ekonomisystem eller branschspecifik programvara, utöver grundläggande felsökning och kontakt med programvaruleverantören;
- support för privata enheter, utöver registrering i Kundens förvaltningsplattform där detta har avtalats;
- arbete på plats, som debiteras per timme med tillägg för resa;
- utbildning utöver kortare vägledning i samband med supportärenden;
- bevakning eller åtgärder utanför supporttid, om inte MDR har beställts enligt punkt 11.6;
- arbete som orsakats av Kundens avtalsbrott eller brott mot Policyn för acceptabel användning, eller av ändringar som Kunden eller tredje part har gjort utan Nord Nodes medverkan; och
- arbete med system som har dokumenterats som undantag enligt punkt 13.

14.2 Arbete som inte ingår kan beställas som Konsulttjänster enligt de priser som anges i Beställningen.

Relaterade dokument

Dokument	Webbadress
Allmänna villkor	https://www.nordnode.se/sv/dam/nordnode/legal/final/document/nordnode-allmanna-villkor-sv.pdf
Personuppgiftsbiträdesavtal	https://www.nordnode.se/sv/dam/nordnode/legal/final/document/nordnode-personuppgiftsbitradesavtal-sv.pdf
Förteckning över underbiträden	https://www.nordnode.se/sv/dam/nordnode/legal/final/document/nordnode-underbitraden-sv.pdf
Servicenivåavtal och supportpolicy	https://www.nordnode.se/sv/dam/nordnode/legal/final/document/nordnode-sla-sv.pdf