

Nordic Training Group

Riktlinje för säker IT- konsumtion Nordic Training Group och dess koncernbolag

DATUM

Utfärdad: 2025-01-10
Gäller från: 2025-01-10
Reviderad: 2026-01-10
Revideras: 2027-01-10

UTFÄRDAD AV

Ansvarig: Joakim Falk
IT-ansvarig
Godkänd av koncernens
ledningsgrupp

SAMMANFATTNING

Detta dokument beskriver riktlinjer som syftar till att stödja en säker IT-konsumtion inom Nordic Training Group och dess koncernbolag.

Dokumentet är ett internt styrdokument.

INLEDNING

Nordic Training Group och dess koncernbolags verksamhet är beroende av information i olika former och åtkomst behöver regleras utifrån gällande informationssäkerhetspolicy.

Denna riktlinje syftar till att stödja en säker IT-konsumtion genom att beskriva och tydliggöra några riktlinjer inom Nordic Training Group och dess koncernbolag.

Denna riktlinje gäller för alla anställda, konsulter, leverantörer och andra tredjepartsanvändare som på något sätt är involverade i Nordic Training Group och dess koncernbolags verksamhet.

Nordic Training Group

ANSVAR

Ledningsgruppen för Nordic Training Group och dess koncernbolag har det övergripande ansvaret för denna riktlinje och dess innehåll.

ÖVRIG ANSVARSBESKRIVNING

Operativ Teamledare IT:

- Arbetet med denna riktlinje och underordnade handlingar.
- Säkerställa kommunikation och utbildning kring denna riktlinje.
- Säkerställa rätt nivå av övervakning och insamling av loggar kring IT-användning, för att säkerställa efterlevnad och minimering av risker kring informationsläckage.

Linjechefer:

- Chefer på alla nivåer har det operativa ansvaret för inom deras avdelning att denna riktlinje introduceras, implementeras och efterlevs.

Medarbetare och konsulter:

- Alla anställda är individuellt ansvariga för att tillämpa reglerna och för att rapportera eventuella överträdelser, incidenter eller brister i riktlinjen.

NORDIC TRAINING GROUPS VÄRDERINGAR OCH DENNA RIKTLINJE

RESPEKT

Vårt IT-stöd skall användas respektfullt och får inte nyttjas för att på något sätt sprida, förvara eller förmedla information som:

- är i strid mot gällande lagstiftning, till exempel hets mot folkgrupp, barnpornografibrott, olaga våldsskildring, förtal, ofredande, dataintrång eller upphovsrättsbrott.
- är att betrakta som politisk, ideologisk eller religiös propaganda.
- är i strid mot gällande lagar kring personuppgiftsbehandling (GDPR).
- är personligt kränkande eller stötande.
- syftar till att marknadsföra produkter eller tjänster som saknar anknytning till Nordic Training Group och dess koncernbolag.
- är i strid mot ingångna avtal.
- stör verksamheten på Nordic Training Group och dess koncernbolag.

EFFEKTIVITET

Rätt använt är vårt IT-stöd ett kraftfullt verktyg för att effektivisera och förbättra medarbetarnas arbete på Nordic Training Group och dess koncernbolag och underlätta i vardagen.

Nordic Training Group

Det innebär att:

- Nordic Training Group och dess koncernbolag kontinuerligt skall söka nya möjligheter att automatisera och förbättra arbetssätt och rutiner med hjälp av vårt IT-stöd.
- Tekniska lösningar skall karakteriseras av hög säkerhet och kvalitet som skall tillgodoses genom kvalitetssäkrad utveckling och standardisering samt att återanvända vedertagna koncept och lösningar.

SAMVERKAN

Ett bra IT-stöd skapar möjligheter att integrera och samverka internt och med andra verksamheter för ökat värde för Nordic Training Group och dess koncernbolag. En stor utmaning är att många av de IT-stöd som används inte kan kommunicera med varandra.

Det innebär att:

- Verksamheten skall tillsammans med IT-stöd skapa säkra möjligheter att samverka på effektivaste sätt både internt och med andra organisationer.

ANSVAR

Nordic Training Group och dess koncernbolag skall ta hänsyn till miljöpåverkan vid planering, införande och användande av vårt IT-stöd, vilket innebära stora möjligheter att bidra till vår omvärlds miljöutveckling.

Det innebär att Nordic Training Group och dess koncernbolag skall:

- beakta miljöpåverkan vid val av nya IT-stöd
- sträva efter att löpande förbättra miljöpåverkan för redan gjorda investeringar.

Alla medarbetare har ett individuellt ansvar att följa denna riktlinje och att tillämpa de regler som definieras här samt att rapportera incidenter och avvikelser mot denna riktlinje.

STRATEGISKA RIKTLINJER

PEDAGOGIK

IT-stöd som pedagogiskt hjälpmedel har en betydande roll i dagens och framtidens utbildningsväsen.

Genom att tillämpa IT-stöd på rätt sätt kan Nordic Training Group och dess koncernbolag bidra till ökade möjligheter för variation och individanpassning för en ökad inläring.

Det innebär att:

- Nordic Training Group och dess koncernbolag skall aktivt nyttja ett IT-stöd på ett sådant sätt att innovativ och effektiv pedagogisk inläring och verksamhet möjliggörs på ett säkert sätt.

SYSTEMSTÖD

Ett av Nordic Training Group och dess koncernbolags strategiska mål, enligt gällande informationssäkerhetspolicy, är att:

- Informationsförsörjningen skall vara säker, effektiv och bidra till stöd åt verksamheterna.

Nordic Training Group

Verksamheten har det yttersta ansvaret för sitt systemstöd och skall ha samordningsansvaret i sina projekt medan IT tillhandahåller resurs enligt behov.

För att nå detta skall utveckling av befintliga eller implementation av nytt systemstöd, ske enligt Nordic Training Group och dess koncernbolags projekt- och förvaltningsmodell.

EFTERLEVNAD OCH UPPFÖLJNING

Två av Nordic Training Group och dess koncernbolags strategiska mål, enligt gällande informationssäkerhetspolicy, är att:

- Informationssäkerhetsarbetet skall ske enhetligt och systematiskt som en naturlig del av verksamheten.
- Händelser i informationssystemen som kan leda till negativa konsekvenser skall identifieras, åtgärdas och förebyggas.

Som en del av arbetet att säkerställa dessa förmågor, etableras insamling av loggar från system inom informationsförsörjningen, för att övervaka aktiviteter ner på individnivå.

DETALJERADE RIKTLINJER

ÄGANDESKAP TILL INFORMATIONEN

Om inte annat är definierat så är utgångspunkten att all information som hanteras inom verksamheten är Nordic Training Group och dess koncernbolags egendom.

DATORER OCH MOBILTELEFONER MED TILLBEHÖR

Personlig utrustning som används i tjänsteutövning skall hanteras på ett säkert sätt som minimerar risken för informationsförluster för Nordic Training Group och dess koncernbolag och generellt gäller:

- Enheten ska skyddas på ett sådant sätt att känslig information inte kommer i orätta händer.
- Enheten ska ha skydd mot skadlig kod och all installerad programvara ska hållas uppdaterad.
- Innehavaren är ansvarig för att spara information på rätt plats utifrån innehåll.
- Säkerhetsuppdateringar, antivirus, säkerhetskopiering av centrala lagringsplatser och IT-system, sköts i normalfallet av IT.
- Utrustningen ska hållas under uppsikt eller vara inlåst.
- Utrustning som inte används ska vara avstängd eller spärrad för åtkomst (t.ex. med lösenordsskydd).
- Fel ska anmälas till ServiceDesk, servicedesk.yrkesakademin@atea.se, 023–58 440.
- Installation och konfiguration av hårdvara får endast göras av IT eller av annan anvisad/auktoriserad person.
- All installation/avinstallation och konfiguration av programvara får endast utföras av IT.

BEHÖRIGHET TILL IT-SYSTEM

Användare ska tilldelas endast de behörigheter som erfordras för att lösa sina arbetsuppgifter enligt principen om minsta möjliga behörigheter som krävs för den aktuella uppgiften.

Detta innebär att användare har behörighet till olika IT-system och olika behörighet för att ta del av

Nordic Training Group

och ändra information i ett IT-system.

- Kontoinformation, så som användarnamn och lösenord, är personliga och får inte lånas ut till annan användare eller administratör.
- Kontoinformation får inte återanvändas för åtkomst till internetplatser som inte är arbetsrelaterade.
- Tilldelning av autentiseringsinformation (t.ex. användarnamn och lösenord) ska ske på ett säkert sätt för att minska risken för spridning och obehörig användning.
- I de fall informationen distribueras via öppna kommunikationssätt t.ex. e-post ska användarnamnet alltid distribueras separat från lösenordet och olika kommunikationskanaler ska användas.
- Närmsta chef är behörig att begära tilldelning eller ändring av behörigheter. Systemägare ska godkänna tilldelning eller ändring av behörighet i respektive system.

LÖSENORDSHANTERING

Alla användare erhåller ett unikt användarnamn och ett tillfälligt lösenord för åtkomst till Nordic Training Group och dess koncernbolags IT-system. Det tillfälliga lösenordet ska bytas till ett personligt vid första inloggningen.

- Lösenord får inte vara detsamma som användarnamnet.
- Lösenord skall bestå av minst åtta (8) tecken varav en stor bokstav och innehålla både siffror och tecken.
- Lösenord får inte vara knutet till personlig information, som till exempel telefon- eller personnummer.
- Lösenord skall bytas ut var 90:e dag.
- Användare som misstänker eller vet att annan person fått tillgång till sitt lösenord skall omgående byta lösenordet.

PROGRAM, LICENSER OCH UPPHOVSRÄTT

Nordic Training Group och dess koncernbolag tillhandahåller licenser för de program som är grundinstallerade i din dator när du får den. Nordic Training Group och dess koncernbolag tillhandahåller även ett utbud av licensierade program och dessa program ska uppdateras regelbundet för att hålla rätt säkerhetsnivå.

Enligt svensk upphovsrättslag är det olagligt att använda eller göra upphovsrättsligt skyddat material tillgängligt utan rättighetsinnehavarens tillstånd. Det krävs att det upphovsrättsligt skyddade material som man laddar ner och kopierar ska vara godkänt av rättighetsinnehavaren.

Brott mot upphovsrättslagen kan innebära att du utsätter både dig själv och Nordic Training Group och dess koncernbolag för civilrättsligt och straffrättsligt ansvar.

MEDVETENHET I PUBLIKA MILJÖER

Anslutning mot trådlösa nätverk utanför jobbet skall göras med försiktighet och använd i första uppkoppling via mobilens abonnemang.

Är detta ej möjligt, säkerställ att tjänsten är säker genom att fråga på platsen där du är vilket nät de tillhandahåller och hur du säkrast kopplar upp dig.

Nordic Training Group

RAPPORTERING AV SÄKERHETSINCIDENTER

Interna IT-säkerhetsincidenter ska omedelbart rapporteras via e-post: helpdesk@ya.se eller via telefon.

Indikationer på att en säkerhetsincident inträffat kan vara att:

- Skyddet mot skadlig kod larmar.
- Datorn utför operationer utan att de initierats (förändringar på skärmen, tecken flyttas eller försvinner).
- Datorn uppträder onormalt (hänger sig, arbetar ovanligt långsamt).

Användare som misstänker att de drabbats av skadlig kod skall:

- Avbryta allt arbete och om möjligt koppla ifrån datorn från nätverket.
- Anteckna vad som hänt (IT-system, tid, felmeddelanden, symtom etc.)
- Kontakta Nordic Training Group och dess koncernbolags helpdesk för rapportering av det inträffade och för att få hjälp med åtgärder för att återställa systemet och förhindra ytterligare skada.