Nordic Training Group

Policy avseende informationssäkerhet

DATUM

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

UTFÄRDAD AV

Ansvarig: Joakim Falk
Operativ Teamledare IT
Godkänd av koncernens ledning

SAMMANFATTNING

Detta dokument beskriver:

- Säkerställande av god informationssäkerhet vid användandet av Nordic Traing Groups system
- Ansvar i organisationen för detta arbete
- Hantering av informationssystem
- Lösenord och systemaccess

BAKGRUND, SYFTE OCH OMFATTNING

BAKGRUND

God informationssäkerhet är en investering samt en billig försäkring och genom att utgå från verksamhetens behov av skyddsnivå kan informationssäkerhetsarbetet ständigt förbättras samt bidra till rätt säkerhetsskydd för troliga och oönskade framtida händelser.

SYFTE

Denna policy anger inriktning och övergripande mål samt säkerställande av ett strukturerat, riskbaserat och konsistent informationssäkerhetsarbete inom koncernen Nordic Training Group.

Syftet är att skydda informationstillgångar från alla typer av hot, såväl externa som interna.

OMFATTNING

Policyn gäller för alla anställda, konsulter, deltagare, leverantörer och andra tredjepartsanvändare som på något sätt är involverade i verksamheten.

INFORMATIONSSÄKERHETS OCH MÅL

INFORMATIONSSÄKERHET

Informationssäkerhet omfattar Nordic Training Group och dess koncernbolags verksamhet och all information utan undantag oavsett den hanteras i cyberrymden, i datorer, i ett telefonsamtal eller på ett papper.

Då stora delar av informationen hanteras med hjälp av IT-system handlar informationssäkerhet även om att kravställa hur våra tekniska lösningar skall fungera.

MÅL

Nordic Training Group och dess koncernbolag har följande mål med sitt informationssäkerhetsarbete:

- Informationsförsörjningen skall vara säker, effektiv och bidra till stöd åt verksamheterna.
- Informationssäkerhetsarbetet skall ske enhetligt och systematiskt som en naturlig del av verksamheten.
- Personal skall ha kunskap kring gällande informationssäkerhetsreglemente och kopplat till de informationssystem/rutiner som används.
- Målsättningen är att informationssäkerhetsarbetet skall följa standarderna ISO/IEC 27001 och ISO/IEC 27002.
- Koncernövergripande rutiner, regler och anvisningar skall upprättas.
- Händelser i informationssystemen som kan leda till negativa konsekvenser skall identifieras, åtgärdas och förebyggas.
- Kontinuitetsplanering skall genomföras för varje informationstillgång för att säkerställa förmåga att bedriva verksamheten på acceptabel nivå under normala förhållanden.

ANSVAR

ÖVERGRIPANDE

Informationssäkerhetsarbete bygger på delaktighet och tydlig ansvarsfördelning samt varje anställds bidrag att tillsammans bygga en säkerhetskultur.

Yttersta ansvaret för informationssäkerheten inom koncernen Nordic Training Group ligger hos koncernens ledningsgrupp.

De beslut som fattas av Dataskyddsombudet för att åtgärda överträdelser av dataskydd måste upprätthållas av företagets ledning.

OPERATIV TEAMLEDARE IT ANSVAR

- Arbetet med denna policy och underordnade handlingar.
- Säkerställa kommunikation och utbildning kring informationssäkerhetsarbetet för alla som omfattas av policy och underliggande dokument.

LINJECHEFERS ANSVAR

- Chefer på alla nivåer inom koncernen har det operativa ansvaret inom sin avdelning att

denna policy med underliggande dokument introduceras och efterlevs.

MEDARBETARENS ANSVAR

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

EFTERLEVNAD

- Eventuella brott mot denna policy kan leda till disciplinära åtgärder.
- Alla incidenter ska registreras och rapporteras samt övervakas kontinuerligt för att identifiera och minimera risker.

HANTERING AV INFORMATIONSSYSTEM

ÖVERGRIPANDE SYFTE

Syftet med att beskriva säker hantering av Nordic Training Group och dess koncernbolags informationssystem är att skydda anställda, konsulter, deltagare, leverantörer, andra tredjepartsanvändare och Nordic Training Group som koncern från illegalt eller skadliga agerande med eller utan uppsåt.

INFORMATIONSSYSTEM

Internet, intranät, datorutrustning, telefon, mjukvara, operativsystem, lagringsmedia (tex USB, hårddisk) och nätverkskonton för email tillhör Nordic Training Group och dess koncernbolag. Dessa system ska primärt användas i verksamhetssyfte och det åligger varje enskild medarbetare att känna till och följa dessa riktlinjer.

LÖSENORD OCH SYSTEMACCESS

LÖSENORD

Lösenord är en viktig del av säkerheten och ett lätt lösenord kan resultera i oönskad åtkomst. Alla användare, inklusive anställda, konsulter, deltagare, leverantörer och andra tredjepartsanvändare med access till Nordic Training Group och dess koncernbolags system är ansvariga för att välja och hantera lösenord som säkrar otillbörlig access.

SYSTEMACCESS

System access ska ges till de system som behövs för att fullgöra befattningsbeskrivning och behörighet ska revideras regelbundet.

ANVÄNDANDE AV INTERNET

SÄKER ANVÄNDNING

IT avdelningen har till ansvar att säkerställa att det finns standarder för system som övervakar och begränsar webanvändning via Nordic Training Group och dess koncernbolags nätverk.

RISK

Felaktig användning kan introducera virus i nätverket.

Nordic Training Group

EMAIL - ANVÄNDNING OCH VIDAREBEFORDRING

SÄKER ANVÄNDNING

Nordic Training Group och bolag inom koncernens varumärken tillhör organisationen och eftersom e-mail bär varumärket i form av e-mailadress och e-mailsignatur är det av största vikt att det används på samma sätt som ett fysiskt brev med företagets logotyp.

Med andra ord ska företagets e-mail bara användas i arbetet och inte privat.

Det är ej tillåtet att sätta upp automatiserad vidarebefordring av mejl från O365 till e-mail adresser utanför Nordic Training Group koncernen.

RISK

Oförsiktig användning av företagets e-mail kan få allvarliga konsekvenser, tex:

- möjligt att skapa legala bindande kontrakt genom att utbyta e-mail
- möjligt att medvetet eller omedvetet skicka känslig information till fel personer
- möjligt att introducera virus i nätverket.

DATORANVÄNDNING

SÄKER ANVÄNDNING

Alla datorer ska låsas när de lämnas oövervakade genom att logga av eller låsa skärmen [Windows-knappen + L]

Undvika användning av lagringsmedia i form av externa hårddiskar eller USB-minnen eftersom de kan komma i orätta händer och utgör en fara om dessa inte är krypterade eller lösenordskyddade.

FYSISK ACCESS

SÄKER ANVÄNDNING

Det är av yttersta vikt att företagets IT system kan fungera stabilt och det är därför vårt ansvar att skydda dessa system från medveten eller omedveten skada samt säkerställa att systemen finns i säkra byggnader och låsta utrymmen med begränsat tillträde.

MOBIL UTRUSTNING OCH TRÅDLÖS ANSLUTNING

SÄKER ANVÄNDNING

IT avdelningen har ansvar att säkerställa att trådlös anslutning kan ske på ett säkert sätt.

RISK

Anslutning till allmänna, öppna nätverk kan innebära stöld av data. Lagring av data på mobilutrustning ökar stöldrisken av enheten.

INSTALLATION AV MJUKVARA

SÄKER ANVÄNDNING

Installation av mjukvara måste godkännas för att minimera oönskade och onödiga problem.

RISK

Installation av icke godkänd mjukvara kan ge problem i form av konflikter med annan mjukvara, introducera virus eller andra program som kan användas för att hacka företagets system och få tillgång till känslig information legal exponering om licenser saknas.

BACKUP OCH HAVERIBEREDSKAP

SÄKER ANVÄNDNING

All data ska hanteras så att det kan skyddas via backup. Det innebär att filer som skapas ska sparas på en nätverksplats eller server.

BACKUP

IT avdelningen måste säkerställa att backup tas regelbundet.

HAVERIBEREDSKAP

Backup ska valideras regelbundet för att säkerställa att den kan användas för att återställa data vid haveri.