IT-sikkerhedspolitik for NH Towage A/S

Formål

Denne IT-sikkerhedspolitik definerer rammerne for NH Towage A/S og forankrer arbejdet i de internationale maritime konventioner, som danner grundlaget for vores drift og sikkerhed, både til søs og på land.

Vi arbejder med IT-sikkerhed som en naturlig del af vores samlede sikkerheds- og kvalitetsarbejde, og som et vigtigt bidrag til at beskytte mennesker, miljø og vores forretning.

Politikken understøtter vores forpligtelser i henhold til internationale maritime konventioner, som danner rammen for sikker skibsdrift og ansvarlig adfærd.

Herunder:

- International Maritime Organisation (IMO)
- Den Internationale Konvention om Eftersøgning og Redning til Søs (SAR)
- Den Internationale Konvention for Sikkerhed for Menneskeliv til Søs (SOLAS)
- Den Internationale Konvention til Forebyggelse af Forurening fra Skibe (MARPOL)
- Den Internationale Konvention om Uddannelse, Certificering og Vagthold for Søfarende (STCW)
- Den Internationale Konvention om Søfarendes Arbejds- og Levevilkår (Maritime Labour Convention, MLC 2006)

NH Towage A/S følger IMO's retningslinjer for håndtering af cyberrisici (MSC-FAL.1/Circ.3. Rev. 3)

IT-sikkerhed til lands og til søs følger GDPR, databeskyttelsesloven samt NH Towage A/S' egne IT-retningslinjer og procedurer.

Gyldighed

IT-sikkerhedspolitikken gælder for alle ansatte i NH Towage og i al anvendelse og adgang til NH Towage A/S' informationssystemer.

Målsætning

NH Towage arbejder aktivt med styring af IT-sikkerhed med det formål at sikre tilgængelighed, integritet og fortrolighed af NH Towage A/S' informationsaktiver, systemer og data.

Til søs: Vi ser it-sikkerhed som en integreret del af maritim sikkerhed og miljøbeskyttelse, i overensstemmelse med kravene i SOLAS, MARPOL og MLC 2006.

IT-sikkerheden i NH Towage A/S følger dansk databeskyttelseslovgivning, GDPR og NH Towage A/S' interne IT-retningslinjer.

NH Towage A/S' anvender en risikobaseret tilgang, hvor beskyttelsesniveauet og omkostningerne hertil skal være baseret på en forretningsmæssig risiko- og konsekvensanalyse som skal foretages minimum årligt.

NH Towage A/S' udarbejder og vedligeholder IT-retningslinjer, som beskriver de konkrete tiltag, krav og procedurer for medarbejdernes brug af IT-systemer i overensstemmelse med denne politik.

NH Towage A/S tilstræber at overholde relevant lovgivning, herunder eksempelvis GDPR.

NH Towage A/S tilstræber at overholde de indgåede aftaler med eksterne parter, herunder databehandleraftaler.

Denne IT-sikkerhedspolitik skal evalueres på årlig basis.

Organisation og ansvar

Bestyrelsen har det ultimative ansvar for IT-sikkerheden i NH Towage A/S.

Direktionen er ansvarlig for styringsprincipperne og delegerer specifikke ansvarsområder for beskyttelsesforanstaltninger, herunder ejerskab af IT-systemer. Direktionen fastlægger hvorledes sikringsforanstaltninger anvendes og administreres i overensstemmelse med IT-sikkerhedspolitikken.

IT-afdelingen, som er ekstern og leveres af Onehouse, rådgiver, koordinerer, kontrollerer og rapporterer om status på sikkerheden.

Den enkelte medarbejder er ansvarlig for at overholde IT-sikkerhedspolitikken og er informeret herom i "IT-anvendelsespolitikken".

Til søs: Skibsføreren har det fulde ansvar og den øverste myndighed til at træffe beslutninger vedrørende sikkerhed, herunder it-sikkerhed, når hændelser påvirker skibets drift eller miljøbeskyttelse.

Dispensationer

Dispensationer til NH Towage A/S' IT-sikkerhedspolitik og retningslinjer godkendes af bestyrelsen ud fra retningslinjer udstukket af ledelsen.

Rapportering

Cyberhændelser behandles som en del af den generelle hændelsesstruktur.

Til søs: Denne hændelsesbehandling gælder ombord, hvor alle sikkerhedsbrud eller cyberrelaterede hændelser skal rapporteres, først telefonisk til den ansvarlige i teknisk afdeling. Derefter udfærdiges Incident Form (Marad) til TEK-afdeling, og behandles efterfølgende ved evaluering på Safety Meeting.

Overtrædelse

Forsætlig overtrædelse og misbrug rapporteres til nærmeste leder og ledelsen.

Overtrædelse af IT-sikkerhedspolitikken eller understøttende retningslinjer kan få ansættelsesretlige konsekvenser.

Afhjælpning og forbedring

Ved konstaterede cyberhændelser eller brud på IT-sikkerheden vil NH Towage A/S straks iværksætte afhjælpning i overensstemmelse med vores procedurer for dialog, genopretning og kompensation.

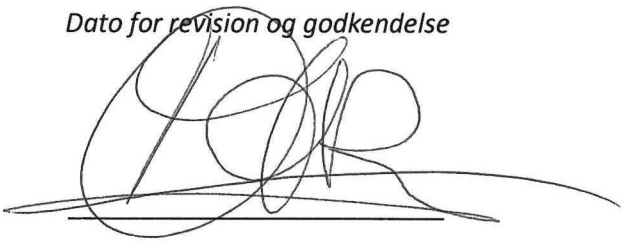
Politikken evalueres mindst en gang årligt og opdateres for at sikre fortsat overensstemmelse med internationale standarder, gældende lovgivning og virksomhedens værdier.

Godkendelse og ikrafttræden

Denne politik er gennemgået og godkendt af NH Towage A/S' øverste ledelse.
Datoen nedenfor angiver seneste revision og ledelsens formelle godkendelse:

18062026

Dato for revision og godkendelse



Niels Henriksen

Owner & CEO

Godkendelse og ikrafttræden

Dokument: IT-sikkerhedspolitik
Version: 1.0
Ikrafttrædelsesdato: 01.07.2026
Seneste revisionsdato: 01.07.2026