IT politikk

Kolos gruppens kjernevirksomhet er spesialkompetanse på materialhåndtering, løfteoperasjoner og løfteutstyr. Vårt tjenestespekter strekker seg fra design og produksjon til inspeksjon og sertifisering.

Våre hovedmål for IT-løsninger:

Kolos gruppen skal ha IT-løsninger som sikrer at informasjon om ansatte, kunder, leverandører, produkter, bedriftens produksjons- og driftsresultater, etc. blir ivaretatt og håndtert på en sikker måte og i henhold til gjeldende regelverk.

Så langt det er mulig skal bedriftens applikasjoner og programvarer være standard, skybaserte løsninger som oppdateres i henhold til gjeldende regelverk og forbedres kontinuerlig av leverandøren.

Bedriften skal ha brannmurer som beskytter nettverket mot angrep, herunder zero-day angrep, virus, brute force innbrudd, botnet, spyware, trojaner, ormer og andre ondsinnede angrep.

Administrasjon av IT-løsningen med tilhørende sikkerhetsvurderinger, oppsett og overvåkning av brannmurer, nødvendige oppdateringer og back-up skal utføres av ekstern leverandør som har spesialkompetanse på området.

Applikasjoner og programvarer skal ha tilgangsstyring slik at tilgang til informasjon kan styres ned på person nivå.

Ansatte er forpliktet til å følge de retningslinjer som er gitt i personalhåndboken, «Kapittel 5 - IT og ID/Adgangskort».

Repr. øverste ledelse i Kolos

Kirsti Tønnessen
Kirsti Tønnessen (Jul 2, 2023 14:42 GMT+2)

Kirsti Tønnessen
Styreleder (Chairman of the Board)

Ansvarlig: Hege Furland		**Godkjent av:** Eivind Windingstad
Versjon: 2	**Sist revidert:** 27.06.2023	**Neste revisjon:**

IT politikk

English version - information purposes only.

Kolos group's core business is specialist expertise in material handling, lifting operations and lifting equipment. Our range of services extends from design and production to inspection and certification.

Our main goals for IT solutions:

Kolos group must have IT-solutions that ensure that information about employees, customers, suppliers, products, the company's production and operating results, etc. are safeguarded and handled in a secure manner and in accordance with current regulations.

As far as possible, the company's applications and software must be standard, cloud-based solutions that are updated in accordance with current regulations and continuously improved by the supplier.

The company must have firewalls that protect the network from attacks, including zero-day attacks, viruses, brute force intrusions, botnets, spyware, Trojans, worms and other malicious attacks.

Administration of IT solutions including security assessments, setup and monitoring of firewalls, necessary updates and backups shall be carried out by an external supplier who has special expertise in the area.

Applications and software must have access control so that access to information can be controlled down to the individual level.

Employees are obliged to follow the guidelines given in the staff handbook, "Chapter 5 - IT and ID/Access card".

Ansvarlig: Hege Furland		**Godkjent av:** Eivind Windingstad
Versjon: 2	**Sist revidert:** 27.06.2023	**Neste revisjon:**