Policy for IT og cybersikkerhet

Ramuddens konsernovergripende retningslinjer for IT, samt informasjons – og cybersikkerhet

DEFINISJON

IT omhandler all teknologi vi bruker for å lagre, behandle og kommunisere med elektronisk informasjon - alt fra maskinvare til programvare.

Cyber-sikkerhet handler om å beskytte selskapets digitale tilganger. Ettersom mer og mer informasjon lagres digitalt og flere og flere arbeidsprosesser blir digitale, øker også risikoen for å bli utsatt for angrep utenfra. Det kan for eksempel være virus, datainnbrudd, sabotasje eller at noen uautoriserte, forsøker å utnytte våre IT-system.

BAKGRUNN

IT gir oss mange fordeler, men eksponerer oss også for risiko. For å øke kunnskapen om IT, redusere risikoen forbundet med IT, og for å skape en klar struktur på hvordan IT styres og brukes i selskapet, er det viktig med felles retningslinjer.

Dessverre risikerer alle bedrifter og organisasjoner å være mål for cyberangrep, både internt og eksternt. Hvis kunders – eller våre ansattes personlige data blir stjålet eller tapt, eller hvis en kunde blir infisert av et virus som kommer fra Ramudden, kan dette alvorlig påvirke både enkeltpersoner og Ramuddens rykte som selskap.

FORMÅL

Retningslinjene som omhandler IT- og cybersikkerhet gir våre ansatte, partnere, leverandører, kunder og andre interessenter en tydelig beskjed på hvordan vi håndterer ulike situasjoner, sammen med de ulike regler og prosedyrer som er gjeldende. De tar sikte på å gjøre oss til gode samfunnsborger, og å styrke Ramudden som selskap. Dette betyr også at den enkelte medarbeider skal føle seg trygg for hva som gjelder hos oss.

RETNINGSLINJER FOR IT OG CYBERSIKKERHET

I de enkelte land, følger Ramudden de lover og forskrifter som er knyttet til IT, og de som er til for å motvirke cyber-kriminalitet. Ved å følge reglene nedenfor, øker vi sjansene for en sikker og tydelig IT-struktur, og reduserer risikoen for at Ramudden skal bli utsatt for angrep eller lignende:

⚠ **Prinsippene** i dette dokumentet, er koblet samme med Ramuddens øvrige retningslinjer og verdier.

⚠ **Usikker på hva som gjelder?**
På detaljnivå kan regler, retningslinjer og prosedyrer variere mellom landene.

Hvis du ikke er sikker på hva som gjelder, ta kontakt med din nærmeste leder, administrerende direktør eller les mer i nasjonale dokumenter.

⚠ **Ramudden-ånden**
Vi følger alle Ramudden-ånden, det vil si at vi har kunden i fokus, setter våre medarbeideres helse og sikkerhet først, og skal være best i det vi gjør. Denne ånden gjennomsyrer også alle vi møter i en profesjonell sammenheng.

Følgelig må alle ansatte til enhver tid følge de lover og retningslinjer som vår virksomhet er underlagt, i enhver oppgave og i ethvert møte, både innenfor og utenfor kontoret.

- **Bruk av IT-utstyr.** Utstyr gjort tilgjengelig av Ramudden (datamaskiner, skjermer, nettbrett, skrivere) er verktøy beregnet for ditt daglige arbeid. Hvis du vil bruke utstyret til privat bruk, spør din nærmeste leder.
- **Programvarehåndtering**. All software/programvare som skal anvendes, må være godkjent av IT-avdelingen, og du må ikke laste ned programvare eller filer uten tillatelse. Piratkopiering er strengt forbudt. Alle datamaskiner må ha godkjente lisenser for den installerte programvaren. Det er heller ikke tillatt å kopiere digitalt beskytte materiale, om dette bryter med loven.
- **Håndtering av E-post.** Alle ansatte har en personlig e-postadresse. Det følger også et ansvar for å sjekke og svare på innkommende e-post, slik at vi alltid skal kunne gi kundene en høy service. Hvis du har fri, er på ferie eller er syk, må du sette opp en fraværsmelding, der du henviser til en annen ansatt som kan besvare henvendelsen.
- **Internett og sosiale medier.** Når du bruker internett på jobben, representerer du Ramudden. Det er derfor ikke tillatt å besøke nettsteder med støtende eller upassende innhold, eller å bruke nett-tilgangen til ulovlige, støtende eller uetiske formål. Det samme gjelder når du bruker sosiale medier; Du får ikke skrive eller gjøre noe som bryter med våre verdier. Selv utenom arbeidstiden, som privatperson, forventer vi at du skal fremstå positiv på internett og i sosiale medier.
- **Datalagring og sikkerhetskopiering.** Bruk bare de datalagringsløsninger som Ramudden tilbyr. Da er filene dine sikre og i tillegg lagres en automatisk sikkerhetskopi av dataene. Det betyr også at Ramudden fortsatt kan beholde viktig informasjon, selv når en medarbeider slutter.
- **Systemtilgang.** Den grunnleggende regelen er at hver enkelt medarbeider bare får tilgang til de systemene som han/hun trenger for å kunne utføre sitt arbeid. Hvis noen får nye arbeidsoppgaver eller slutter, er nærmeste lederen ansvarlig for å endre systemtilgangen.
- **Mistede enheter eller virus**. Våre ansatte må ta en aktiv rolle i IT- og nettverkssikkerhet. Ansatte som har bærbare datamaskiner må være ekstra forsiktige - la den aldri ligge igjen i bilen eller lignende, da den er et attraktivt objekt for tyveri og fordi informasjonen på den, er kritisk for oss.

  Hvis du har mistet eller blitt bestjålet enheten din, eller hvis du mistenker at den er infisert med virus, må du kontakte din IT-avdeling umiddelbart eller eventuelt IT-støtten i ditt land.

⚠

Viktige huskeregler

- Del aldri kredittkort-opplysningene dine, selv om e-posten eller forespørselen på internett ser ut til å komme fra en kollega.
- Del aldri passordet ditt. Hvis du virkelig må, så gjør det personlig eller via telefon i stedet for i en e-post.
- Skriv aldri passordet ditt på en post-it-lapp på datamaskinen din. Husk det i stedet!
- Klikk aldri på koblinger i en e-post hvis du ikke stoler på avsenderen.
- Lås alltid datamaskinen når du forlater arbeidspulten.
- Hvis du bruker Ramuddens e-post på mobil eller nettbrett, må du beskytte enheten med en PIN-kode eller ved å bruke fingeravtrykk – ID.

ANSVAR

Alle ansatte er personlig forpliktet til å overholde alle lover, forskrifter, myndighetskrav og retningslinjer som er knyttet til IT og cybersikkerhet. Å bryte retningslinjene kan innebære disiplinære sanksjoner. Til syvende og sist er det Ramuddens ledere som er ansvarlige for at retningslinjene er kommunisert til de ansatte, og til relevante eksterne parter, for å fremme en bredere kunnskap om og bruk av disse retningslinjene.

➔ Mistenker du at IT-strukturen eller cybersikkerheten i noen henseender er truet? Ta da kontakt med din nærmeste leder, administrerende direktør eller personalavdelingen.

⚠

Selv på nettet representerer du Ramudden!

Når du bruker Ramuddens IT-utstyr og for eksempel surfer eller kommentere i sosiale medier, gjør du det som en Ramudden-ansatte.

Den grunnleggende regelen er at du aldri skal gjøre noe på nettet som du ikke ville gjøre "i virkeligheten".

⚠

Det er et utarbeidet et særskilt dokument for retningslinjer og bestemmelser knyttet til GDPR.