Retningslinjer for brug af IT

Indhold

Generelt

Retningslinjer for brug af IT er gældende for alle ansatte, leverandører og vikarer i EWII, altså alle som benytter EWIIs systemer. Det er nærmeste leders ansvar, at de pågældende er orienteret herom.

Chefen for de enkelte afdelinger har ansvaret for, at retningslinje for brug af IT overholdes. Ved konstatering af overtrædelser, skal der rapporteres til nærmeste leder, den IT-sikkerhedsansvarlige eller IT-chefen.

Den IT-sikkerhedsansvarlige er ansvarlig for, at retningslinjerne ajourføres. Retningslinjerne skal som minimum revideres årligt.

Ansvarsområder

IT-afdelingen er ansvarlig for og skal sikre, at

- din PC fungerer korrekt og har installeret EWIIs standardprogrampakker, så du altid kan løse dine arbejdsopgaver.
- der tilbydes professionel IT-rådgivning og IT-projektdeltagelse/ledelse.
- der tilbydes hurtig og effektiv information om IT-servicearbejde og evt. driftsforstyrrelser.
- der tilbydes forretningsorienteret rådgivning ved IT-relaterede indkøb. Herunder også rådgivning omkring datasikkerhed.
- oppetid og driftsstabilitet på alle IT-faciliteter og IT-systemer er i henhold til den indgåede administrationsaftale.
- din PC og e-mailkonto er sikret bedst muligt mod virus- og malwareangreb. Vær opmærksom på at IT ikke kan sikre dette 100%, det er samtidig også din opgave at sikre dette.
- du har adgang til netværksprinter fra din PC.
- dine data og filer på EWIIs servere er sikret ved backup.
- de fra EWII udleverede smartphone, tablet og PC fungerer korrekt.
- reparere eller udskifte din PC og andet udleveret IT-udstyr, hvis det går i stykker, i forhold til administrationsaftalen.
- der tilbydes support med venlig, hurtig, målrettet og problemløsende sagsbehandling i administrationsaftalen.
- du får rettigheder til data/filer/drev, der er relevant for løsningen af dine arbejdsopgaver hos EWII.
- der kan understøttes kryptering når der er et forretningsmæssigt behov

Som medarbejder er du ansvarlig for og skal

- gøre sig bekendt med og overholde EWIIs retningslinje for brug af IT.
- altid gemme dokumenter og data i EWIIs dokumenthåndteringssystem (DocuNote)
- anvende Helpdesk til bestilling af IT-udstyr og software
- holde en stram datadisciplin og er ansvarlig for at data er valide.
- arkivere alle e-mails, af forretningsmæssig karakter, i DocuNote eller lignende værktøjer benyttet hos EWII.
- orientere sig om nyheder og ændringer på ROFERT.
- bruge IT-systemer med omtanke og på en sikker måde.
- rapportere fejl, uhensigtsmæssigheder og ønsker på IT-området til Helpdesk.
- vedligeholde og udbygge sine IT-kompetencer.
- bidrage til vidensdeling og hjælpe kolleger med brugen af IT.

- fokusere på høj datakvalitet, dvs. skabe troværdige og aktuelle data, dokumenter og informationer.
- Må ikke installere uautoriserede programmer på EWII udstyr, der må kun benyttes software som er godkendt af IT-afdelingen.
- Må ikke afinstallere/deaktivere sikkerhedsprogrammer og features herunder firewall og anti-virus.
- gøre sig bekendt med, at alle dokumenter og data, der er fremstillet i forbindelse med udførelse af arbejdet, er EWIIs ejendom.
- ikke lagre data permanent på USB-drev, lokaldrev eller på PC's skrivebord, dette må kun gøres midlertidigt. Der tages ikke sikkerhedsbackup af USB, lokaldrev og PC's skrivebord.
- ikke lagre billeder, musikfiler, video/film og lignende på EWIIs udstyr, som ikke er relevant for arbejdets udførsel.
- anvende Helpdesk til registrering af opgaver. Ved hasteopgaver kan telefonsupport-nummeret anvendes i forhold til SLA.
- være opmærksom på, at adgang til data og systemer kun sker i forhold til "need to have" og ikke "nice to have".
- ikke benytte cloud løsninger uden godkendelse.

IT-afdelingen tilbyder, at gæster og samarbejdspartnere

- kan få Internetadgang med et gæste-id. Gæste-login udleveres i receptionen.

Gæster og samarbejdspartnere skal overholde gældende retningslinjer for brug af IT. Samarbejdspartnere, der skal tilgå EWIIs systemer, skal gøre dette fra udleveret EWII udstyr eller via Citrix. Samtlige samarbejdspartnere skal underskrive tro og love-erklæring eller databehandleraftale.

Sikkerhed

- er også dit ansvar!

IT-sikkerhed bliver du først opmærksom på, når det ER gået galt - når du sletter dokumentet ved et uheld, eller computeren bliver lukket ned af en virus, mens du har allermest travlt. Viden og omtanke kan redde dig fra mange ærgrelser og spildt arbejdstid.

Det stærkeste kort i beskyttelsen af din computer og dine vigtige dokumenter er faktisk din sunde fornuft, så du behøver ikke at være ekspert!

Brug en sikker adgangskode

Adgangskoden er den vigtigste beskyttelse mod misbrug af din digitale identitet og personlige data. Vælg den med omhu. Adgangskoden skal herefter overholde følgende regler:

Overordnede regler for adgangskoder

- Adgangskoder er personlige og må ikke deles med andre personer.
- Hvis der er mistanke om, at andre kender ens adgangskode, skal adgangskoden ændres øjeblikkeligt.
- Adgangskoder må ikke benyttes på tværs af systemer. Dette betyder, at hvis en adgangskode benyttes til Windows, må denne adgangskode ikke genbruges i andre systemer eksempelvis energinets beredskabsside eller din personlige Facebook konto.

- Adgangskoder må ikke genbruges på tværs af konti. Dette betyder, at brugere med en alm. Brugerkonto og en Administrativ brugerkonto, ikke må benytte samme adgangskode for de to konti.
- Adgangskoder som benyttes privat må ikke benyttes på EWIIs systemer.
- Der må ikke benyttes fortløbne numre, eksempelvis EWii!!10, EWii!!11, EWii!!12 osv.
- Adgangskoder må ikke indeholde fornavn, virksomhedsnavn eller brugernavn.
- Det er ikke tilladt at skrive adgangskoder ned, det gælder både fysisk og digitalt. Med mindre den digitale løsninger er krypteret på en sikker måde. Digitale løsninger skal godkendes af EWIIs IT-afdeling.
- Der må ikke benyttes keyboard-walks, dette betyder sammenhængende karakterer på tastaturet. Eksempelvis qwerty12345.

Adgangskodekrav

Adgangskodekravene opdeles i forskellige roller, herunder

- Alm. Bruger. De brugere som ikke er en del af nedenstående grupper.
- Brugere med adgang til følsomme oplysninger, herunder følsomme persondata.
- Brugere med adgang til kritisk infrastruktur.

Almindelige brugere

- Antal tegn: minimum 8 karakterer
- Skal overholde tre ud af fire følgende:
    - Store bogstaver
    - Små bogstaver
    - Tal
    - Specialtegn
- Skal skiftes hver 120. dag

Har du som medarbejder adgang til personfølsomme oplysninger og kritisk infrastruktur, skal der benyttes en adgangskode på minimum 16 karakterer.

Se evt. beskrivelse på Rofert om, hvordan man vælger en stærk adgangskode.
http://rofert/IT/Lists/Nyheder/DispForm.aspx?ID=397&Source=/Sider/Startside.aspx

Hvordan vælges en god adgangskode

Der er mange metoder til at vælge en god adgangskode, og det er vigtigt at fokusere på, at det er længden af adgangskoden, som giver den største sikkerhedsmæssige værdi.

En god metode til at vælge adgangskode er at sammensætte fire ord og derved generere en adgangskode ud af disse. Dette kan eksempelvis være:

”Fodbold246810SommerferieDoerhåndtag”

På denne måde kan man lave en adgangskode på 34 tegn, som også er let at huske.

En sidste bemærkning, anvend ALDRIG de eksempler, som er givet i vejledningen. Find i stedet på jeres egne og personlige variationer.

Håndter vedhæftede filer med omtanke

E-mail, Skype, Messenger eller andre kommunikationskanaler kan indeholde vedhæftede filer eller links, du ikke bør åbne eller se på. Sund skepsis er dit bedste forsvar. Pas på spam og phishing – fjendtlig kommunikation.

E-mails eller anden kommunikation du modtager, som du ikke kender afsender på, skal du ikke åbne, hvis du er i tvivl.

Links, som ikke kan forbindes med arbejdsrelaterede opgaver, må ikke åbnes.

Hvis du modtager e-mails eller anden kommunikation, som du mener kan være fjendtlig kommunikation, så underret helpdesk. På denne måde kan helpdesk være proaktiv og sikre at andre af dine kollegaer ikke ved et uheld kommer til at klikke på ondsindede links eller filer.

Lås din pc, når du forlader den

Selv den bedste adgangskode er nytteløs, hvis du går fra din maskine uden at låse den.

E-mail kommunikation

E-mails er en integreret del af den daglige kommunikation internt og eksternt. Samtidig er en e-mail lige så forpligtende som et brev.

Alle, der har en e-mailadresse, er forpligtet til at gennemgå postkassen dagligt.

Hvis du er fraværende, skal du sørge for, at der automatisk sendes et kvitteringssvar til afsender med besked om, at der er tale om et autosvar, at du ikke er til stede, hvornår du kommer tilbage, og hvem afsenderen evt. kan henvende sig til i stedet for.

Det er vigtigt, at modtageren hurtigt og let kan identificere såvel budskab som afsender. Derfor skal e-mails fra EWII som udgangspunkt have hvid baggrund, dvs. ingen farver eller mønstre. Afsendersignatur skal benyttes til ekstern kommunikation.

E-mailen må desuden ikke indeholde kampagnebanner eller lignede illustrationer, jf. Markedsføringsloven § 10.

Du skal anvende e-mails med omtanke og respekt for EWIIs værdier og du skal behandle e-mails på samme måde som anden korrespondance.

Personfølsomme oplysninger, CPR numre, oplysninger omkring kritisk infrastruktur og andre følsomme oplysninger må som udgangspunkt aldrig sendes over E-mail. Hvis der er et forretningsmæssigt behov for dette, skal det gøres krypteret.

Outlook kalender

Det er vigtigt at du har din Outlook kalender åben for kollegaer og ajourfører den løbende. Dette er en stor hjælp for receptionens muligheder for god kundeservice, og for at få en effektiv mødetilrettelæggelse. Husk at private aftaler skal markeres som privat, da din kalender jo som udgangspunkt er åben.

USB-Nøgler

USB-Flashdrev (almindeligvis kendt som "USB-stick/USB-nøgle") har stigende lagerkapacitet og er særligt velegnede til overførsel af data fra en computer til en anden uden behov for at forbinde de to computere.

Imidlertid er sådanne anordninger særligt tilbøjelige til at blive tabt og mistet, hvilket kan føre til tab eller kompromittering af data. Alle data, der holdes på USB-Flashdrev, må kun være midlertidigt til det specifikke forretningsformål med overførsel af data. Permanent eller langvarig opbevaring af kritisk data på USB-Flashdrev er ikke tilladt. Det anbefales at der kun benyttes krypterede USB-Flashdrev.

Hvis USB-Flashdrev benyttes til personhenførbare oplysninger eller oplysninger omkring kritisk infrastruktur SKAL disse være krypteret. Husk at følge de gældende regler for adgangskoder når der skal vælges adgangskoder til den krypterede enhed.

Der findes en vejledning til hvordan man krypterer og benytter krypterede USB-nøgler. Denne kan findes under Guides (Kryptering af USB-nøgler) ved at benytte følgende link:
http://rofert/IT/Guides/Forms/AllPages.aspx

Brug af Internet

Acceptabel brug

- Adgang til internettet til legitime forretningsformål betragtes som acceptabel brug.
- Derudover kan du lejlighedsvis tilgå internettet til personlig brug, som personlig e-mail, rejse, læge osv. Du skal bruge din fornuftige vurdering af, hvad der er lejlighedsvis adgang, men det skal være baseret på minimal adgang til de websteder og tjenester, der er nødvendige for det daglige liv, der på ingen måde forstyrrer at opfylde din rolle inden for EWII (enten hvad angår adgang til tjenester eller tid brugt).

Følgende anses for uacceptabel brug, uanset om det er af forretningsmæssige eller personlige årsager:

- Enhver aktivitet, der kan negativt påvirke eller skade EWIIs omdømme
- Downloade eller installere software, som ikke er godkendt af IT-afdelingen
- Etablere forbindelse til andre virksomhedsnetværk uden tilladelse fra IT-afdelingen.
- Tilslutte udstyr (ikke af IT-afdelingen udleveret udstyr) til netværket, herunder også leverandørers udstyr.
- Omgå systemer som er etableret til at beskytte personfølsom data eller anden følsom data
- Surfe på hjemmesider, som indeholder: Sex, porno, vold, opfordrer til vold og ulovligheder eller sider, som har til hensigt at skade eller nedværdige personer.
- Foretage ulovlige transaktioner (søgninger).
- Udgive sig for andre personer (bruge forkert e-mail/navn).
- Kopiere fortroligt materiale til/fra EWII, som ikke er relevant for udførslen af dit arbejde.
- Kigge på, ændre eller bruge andres filer uden at have deres fulde tilladelse.
- Sende/modtage fortrolig info om EWII.
- Bruge internettet til privat vinding (hente/skrive oplysninger/filer, så man privat modtager penge).
- Sende personer/firmaer uopfordret e-mail og reklamer.
- Personfølsomme oplysninger eller følsomme oplysninger omkring kritisk infrastruktur må aldrig uploades til Internettet.

Brug af sociale medier

Al brug af kommercielt tilgængelige webbaserede e-mail- og sociale netværkskommunikationsapplikationer skal være i overensstemmelse med gældende lovgivning. Desuden:

- Kommercielt tilgængelige e-mailapplikationer, herunder men ikke begrænset til Gmail, Yahoo!, Hotmail etc. må kun bruges til personlig kommunikation. Personhenførbare oplysninger eller følsomme oplysninger omkring kritisk infrastruktur må aldrig sendes over disse medier.
- Kommercielt tilgængelige sociale netværksapplikationer, herunder men ikke begrænset til Twitter og Facebook, må kun bruges til personlig kommunikation i overensstemmelse med HR's retningslinjer, medmindre det kræves som en del af en arbejdsopgave. Personhenførbare oplysninger eller følsomme oplysninger omkring kritisk infrastruktur må aldrig sendes over disse medier.
- Kommerciel tilgængelig (ikke-administreret af EWII) webbaserede Instant Messaging-applikationer, herunder men ikke begrænset til Microsoft Communicator, Skype og Yahoo!, må kun bruges til personlig kommunikation. Personhenførbare oplysninger eller følsomme oplysninger omkring kritisk infrastruktur må aldrig sendes over disse medier.

Beskadigelse, tab og tyveri af udstyr

Sørg for at udstyret behandles og opbevares, så tyveri, tab og beskadigelse forhindres bedst muligt. Ved tyveri eller tab af IT-udstyr anmeldes det straks til IT-afdelingen, dette inkluderer også tyveri eller tab af USB-nøgler.

Husk altid at slukke din bærbare PC når du forlader den, det er ikke nok at klappe den sammen. Ved at gøre dette besværliggøres indbrud og datatyveri.

Lad ikke udstyr ligge synligt i bilen, hvis du forlader den.

Brug af eget IT-udstyr

Det er ikke tilladt at benytte eget udstyr på EWII netværk, eget udstyr må kun benyttes på EWIIs gæstenetværk.

Når der arbejdes fra andre lokationer end EWII, skal det sikres, at samme niveau af sikkerhed benyttes. At der eksempelvis ikke printes dokumenter med følsom information som ligges fremme.

Logning af e-mail og internettrafik

EWII logger al internettrafik og e-mails, der sendes fra EWII og tilgår EWII af hensyn til drift, sikkerhed, genetablering af dokumenter og dokumentation samt kontrol af medarbejdernes brug.

Internetlogningen består i registrering af dato og klokkeslæt for søgningen på internettet, IP-adressen, http-adressen og fejlkoder.

E-mail logningen består i registrering af afsender, modtager, emne på e-mailen og indhold.

EWII forbeholder sig ret til at foretage stikprøvekontrol af logning af e-mail og internettrafik i forhold til de nedenfor nævnte hensyn. Stikprøvekontrol kan foretages både generelt i forhold til trafik og konkret i forhold til enkeltpersoner.

Hvis forbrug afviger fra det normale, eller der er andre forhold, som fx mistanke om misbrug, der medfører behov for det, kan ledelsen til enhver tid iværksætte en kontrol af, om retningslinjerne overholdes.

IT-chefen kan, efter godkendelse fra direktionen, åbne e-mail og eventuelle vedhæftede filer, kalender og skaffe sig indsigt i enhver færden på internettet, hvis og i det omfang dette er påkrævet i forbindelse med en kontrol. Dette gælder ikke private e-mails, når det tydeligt fremgår af disse, at de er private.

Herudover vil kontrol ske, hvor EWII vurderer behov herfor til varetagelse af de ovennævnte hensyn. Hvis misbrug skønnes at have fundet sted bliver medarbejderen kontaktet. Direktionen orienteres med det samme om ethvert muligt misbrug.

Overtrædelse af reglerne kan få konsekvenser for ansættelsesforholdet.

EWII forbeholder sig ret til at indberette ulovligheder til rette myndigheder.

Sikker bortskaffelse og genbrug af udstyr

Al udstyr udleveret fra IT-afdelingen, skal leveres tilbage, når og hvis dette ikke skal benyttes længere, dette gælder også USB-nøgler og andre lagermedier.