25d

Förslag till användarpolicy gällande IT och Telefoni

KONGRESS 2025

seko

Stockholm maj 2025

Användarpolicy gällande IT och Telefoni

Inledning

Denna policy beskriver allmänna och individuella regler för dataskydd och informationssäkerhet samt förhållningssätt vid användning av all IT och telefoni. Alla som arbetar med, och använder, organisationens information och IT-utrustning, såsom datorer, telefoner och surfplattor, omfattas av denna policy.

Den IT-utrustning som tillhandahålls inom ramen för verksamheten är organisationens egendom. Den är till för att stödja och effektivisera arbetet och underlätta kommunikationen för anställda och förtroendevalda.

IT-utrustning och tjänster

All utrustning som ägs av organisationen är avsedd för användning kopplad till anställningen eller förtroendeuppdraget och är att anses som personlig utrustning, dock inte privat, och får endast nyttjas av den anställde/förtroendevalde och inte av annan person. Reglerna för användning, hantering, säkerhet och återvinning gäller all IT utrustning.

IT-utrustningen är ett viktigt och kostsamt arbetsredskap och ska därför hanteras varsamt. För att skydda utrustningen ansvarar användaren för att den alltid är skyddad med särskilt skyddsskal, fodral eller väska. Beslut om byte av IT-utrustning fattas av IT-samordnaren i samråd med närmsta chef. Inköp sker enligt gällande inköpsreglemente.

Förbundet står för service och reparation av skador på all utrustning som tillhör förbundet. Vid upprepade skador, grov oaktsamhet, eller där skydd på tex mobiltelefon inte används kan den anställde/förtroendevalde bli betalningsskyldig för service och reparation via avdrag på nettolön/uppdragsredovisning.

Återlämning

All IT-utrustning skall återlämnas till organisationen vid anställningens eller uppdragets upphörande. Mobiltelefon och eventuell surfplatta skall återställas och Apple ID loggas ut så att telefonen kan användas av annan person, innan den lämnas till närmsta chef/IT-samordnaren. Detta gäller även vid utbyte av IT-utrustning. Utrustning innehållande lagringsmedia kommer att förstöras alternativt rensas på information i syfte att ingen information kommer på avvägar.

Regler IT-utrustning och tjänster

- Varken organisationen, FASAB eller dess driftpartner får stängas ute från innehållet genom kryptering eller liknande.
- Användning av tillhandahållna IT-resurser får inte strida mot förbundets mål eller skapa dåligt anseende.
- Upphovsrättsskyddat material som ej tillhör arbetsgivaren som till exempel bilder, filmer, dokument eller programvara får inte lagras på arbetsgivarens utrustning.

- Privat användning får inte medföra kostnader för förbundet genom t ex kapacitetsproblem.
- Surfande på kriminella, rasistiska, pornografiska eller liknande hemsidor är förbjudet. Undantaget de anställda där det ingår i den anställdes arbetsuppgifter och är sanktionerat av närmsta chef.
- E-postadressen tillhandahållen av förbundet får ej användas för privat bruk.
- Det är inte tillåtet att spara arbetsrelaterade dokument eller bilagor på en annan enhet/molntjänst än den som tillhandahållits av organisationen.
- En trasig dator, telefon eller surfplatta ska i första hand repareras om reparationskostnaden anses skälig i förhållande till kvarvarande livslängd på utrustningen. Det är IT-samordnaren i samråd med närmsta chef som tar beslut om ny utrustning ska inhandlas.

Tillgång till vissa system så som Puma, e-post och lagringsytor i M365 kommer att vara begränsad till länder inom EU. Vid resor i tjänsten utanför EU, kan Fasab Servicedesk lägga till personen i en särskild säkerhetsgrupp, ”Tillåtna resenärer”, under tiden resan utanför EU sker och man har då fortsatt tillgång till våra olika system.

Telefoni

- Mobiltelefoner inköpta av förbundet skall vara managerade med av FASAB tillhandahållna verktyg.
- Telefonitjänster (exempelvis samtal, mobilt data, SMS, MMS) är avsedda för användning i tjänsten men får även användas för privata ändamål inom EU så länge det inte inkräktar på arbetets utförande eller genererar kostnader för arbetsgivaren. Betaltjänster där kostnaden hamnar på telefonräkningen, till exempel sms-biljetter, parkeringsavgifter, Blocket annonser, röstningar eller tävlingar mm får inte användas för privat bruk.
- Vid vistelse utanför EU ska mobiltelefoni och datatjänster användas sparsamt och inte medföra oskäliga kostnader. Uppkoppling mot färjors/kryssningsfartygs egna satellituppkopplade mobilnät är inte tillåtet med organisationens utrustning då kostnaderna är mycket höga, både för samtal, sms och datatrafik.
- Appar skall laddas ned med försiktighet. Organisationen står inte för kostnader av köp av appar eller lagringsutrymme etc.

Säkerhet

Organisationens IT-utrustning såsom mobiltelefoner, surfplattor och datorer utgör en allt större risk för förbundet. Det är därför viktigt att alla användare följer de säkerhetsrutiner och riktlinjer som förbundet beslutat om. Det är användarens ansvar att känna till dessa riktlinjer och regler.

- Extern lagringsmedia (ex USB, extern hårddisk) får ej användas på organisationens datorer.
- Tveksam e-post öppnas inte utan slängs direkt. Därefter töms papperskorgen. Om man är osäker på huruvida ett e-post-meddelande innebär en säkerhetsrisk eller inte bör man alltid vända sig till närmsta chef, IT-samordnaren eller Fasab Servicedesk för råd och vägledning.
- Privata backuptjänster såsom Onedrive, Dropbox, Google Cloud eller liknande är ej tillåtna att lagra organisationens data på.
- Dator, surfplatta eller mobiltelefon ska ej lämnas utan uppsikt i olåst läge.
- Användare med av förbundet inköpt mobiltelefon ansvarar för att verktyget för managering av mobiltelefon är installerat på enheten.
- Borttappad eller stulen IT-utrustning ska omgående anmälas till Fasab Servicedesk, polis och till IT-samordnaren.
- Som användare ska du löpande ta del av den information och de utbildningar som Fasab eller förbundet tillhandahåller när det gäller IT, dataskydd och informationssäkerhet.

AI

Det är inte tillåtet att använda externa AI verktyg där organisationens data eller personuppgifter matas in i tjänsten. Exempel på organisationens data är kollektivavtal, stadgar, policys, riktlinjer, organisationsschema, protokoll etc. Fasab utför dataskyddsprövning på programvaror och tjänster som förbundet använder. Av den anledningen bör endast godkända AI-verktyg användas i arbetet och i det fackliga uppdraget.

Incidentrapportering

Varje användare är skyldig att rapportera upptäckta problem, hot, överträdelser, svagheter och andra handlingar som bryter mot policys, riktlinjer och instruktioner. Händelser som bedöms hota informationssäkerheten ska rapporteras omgående till Fasab Servicedesk.

Hantering av personuppgifter

Som anställd eller förtroendevald har du en skyldighet att behandla personuppgifter i enlighet med förbundets kommunicerade instruktioner, detta gäller både vid spridning och framför allt av rensning av personuppgifter när syftet med hanteringen inte längre kan motiveras.

Varje användare är skyldig att rapportera misstänkta personuppgiftsincidenter till *gdpr@seko.se*.

Kontroll

Seko kontrollerar inte sina anställda eller förtroendevaldas arbetsinsats via datasystem, vare sig kvantitativt eller kvalitativt, utan att arbetstagarna känner till det.

Vid fara för informationssäkerhet, t.ex. vid virus eller hackerangrepp, eller om det finns välgrundad misstanke om att en anställd/förtroendevald gjort sig skyldig till sådan handling som är grund för arbetsrättsliga åtgärder kan förbundet komma att begära ut innehåll i dokument, e-post och loggar. Vid misstanke om brott görs polisanmälan.

Vem ansvarar för att policyn efterlevs?

Förbundsstyrelsen är ytterst ansvarig för att regler och riktlinjer efterlevs.

Om det framkommer att dessa regler och riktlinjer överträtts kan det komma att utredas. Seko kommer i första hand försöka åstadkomma rättelse genom påpekanden eller liknande förfaranden. Vid allvarligare missbruk kan arbetsrättsliga åtgärder komma att vidtas. Användare kan även stängas av från att använda Sekos IT-utrustning och IT-system.


seko