2023-06-20

POLICY

# Informationssäkerhet

(Beslutad av förbundsstyrelsen 230620 och ersätter tidigare godkänd policy daterad 210323)

Fackförbundet ST är en organisation med stor tillgång till IT-resurser som stöd för att utföra sina arbetsuppgifter och uppdrag. Det innebär möjligheten att använda Internet, e-post, verksamhetssystem och att komma åt Fackförbundet STs intranät med mera. Detta innebär också ett personligt ansvar för att upprätthålla säkerheten.

### Denna policy redovisar de villkor som gäller för användning av IT i STs verksam­het och syftar till att:

* säkerställa en tillräcklig hög IT-säkerhet,
* säkerställa god kvalitet på information och
* informera om regler för IT-användning.

Att skydda förbundets information är viktigt och något som ligger i samtligas intresse. Därför förutsätts det att alla med­verkar i säkerhetsarbetet och följer nedan angivna riktlinjer vid all IT användning för att skydda samtliga användares och registrerades integritet.

### Riktlinjer

Datorer och mobiler som anskaffats av ST är avsedda att användas i tjänsten/uppdraget. ST äger all information som framtagits i eller i anslut­ning till tjänsten. ST ska ha obegränsad tillgång till informationen och får inte utestängas från innehållet genom kryptering eller liknande.

Fackförbundet STs IT-funktion har rätt och skyldighet att kontrollera att utrustning fungerar. All information i enheter kan därför komma att kontrolleras. Även av andra skäl kan det finnas anledning att gå igenom och kontrollera datorer och mobiler, till exempel för att hitta virus- och hacker­an­grepp. Om det finns olagliga bilder, piratkopierat material eller liknande kan det medföra juridiska konsekvenser för ST.

**Privat användning**

Privat användning (surfande på Internet, användning av sociala medier, e-post, samtal, lagring av privata do­kument mm) ska ske med gott omdöme och ej under arbetstid. Privat använd­ning av datorer och mobiler får ej medföra merkostnader för ST genom till exempel kapacitetspro­blem av att enhetsminnet fylls, att kommunikationstider försämras eller att den av ST betalda surfmängden på mobiler förbrukas.

Det är inte tillåtet att:

• Ringa betalsamtal (riktnr 071, 0900, 0939, 0944)

• Betala lokaltrafik, parkering eller liknande med betal-sms

• Ringa röstningssamtal (riktnr 099)

Om detta ändå av någon anledning sker så är det användarens ansvar att meddela Ekonomi- och service (ekonomi@st.org) om detta för att reglering av privat kostnad ska kunna hanteras.

**Internetanvändning**

Det är förbjudet att använda STs utrustning för att avsiktligt besöka rasistiska eller pornografiska webbsajter. Det är inte heller tillåtet att skicka e-post från sitt ST-konto som kan uppfattas som kränkande eller stötande. När man använder arbetsutrustning står alltid ST som avsändare om en enskild förtroendevald/medarbetare deltar i chatt-grupper, använder sociala medier eller skriver in­sändare.

**E-post**

Utöver denna policy omfattar STs mål all kommunikation i förbundet vilket kräver kontinuerlig bevakning av e-post, Teams med mera.

Alla anställda ansvarar för att den egna brevlådan kontinuerligt avläses och besvaras. Svar eller bekräftelse på att e-post emottagits ska skickas senast vardagen efter att e-posten tagits emot. Även ett autosvar räknas som bekräftelse. Svara ska vi alltid göra så skyndsamt som det bara är möjligt.

På mobiler ska Outlook användas för att hantera arbetsmejl och kalender – då skyddas innehållet av våra säkerhetssystem. De mejl- och kalender- appar som finns i telefonen får inte användas för att hantera arbetsmejl mm – men kan användas för privata saker.

Autosvar är att rekommendera om man är mycket uppbokad och vet med sig att det kommer ta mer än ett dygn innan man kan svara ordentligt. Vid ledighet ska autosvar alltid ställas in.

Se till att Outlook-kalendern är uppdaterad och svara alltid på möteskallelse så snart som möjligt.

Att skicka privat e-post från förbundets e-post-system bör undvikas eftersom förbundet står som avsändare. Även pri­vat surfande från ST utrustning sker i förbundets namn. Detta är viktigt att tänka på då man vid allt surfande lämnar elektroniska spår efter sig på besökta sidor.

Om du skickar känslig information med e-post - tänk på att informationen är lätt åtkomlig och även lätt att ändra/förvanska.

**E-post för förtroendevalda**

Förbundet erbjuder en mejltjänst för förtroende via förbundets driftleverantör, HPS. Mejltjänsten är helt skild från förbundets egna system och tillhandahålls av HPS som ansvara för allt kring tjänsten (support, behörigheter, konto mm).

Förtroendevalda uppmanas att inte använda gratis mejltjänster (dels pga GDPR) och att anända arbetsgivarens kan vara problem vid ev. konflikt och även pga GDPR då arbetsgivaren inte vill vara ansvarig för medlemsinformationen som ev. lagras i mejlsystemet.

**Mjukvara**

Fackförbundet ST stödjer Business Software Alliance vilket innebär att enbart licenserade program får användas inom förbundet. Det är brottsligt att använda piratkopierad mjukvara och missbruk kan innebära böter och fängelsestraff. Det är inte tillåtet att använda piratkopierad mjukvara på någon utrustning som tillhör ST. Kontakta IT-funktionen vid frågor om programlicenser.

För att minimera virusrisken ska försiktighet råda vid nedladdning av filer. Det är förbjudet att ladda ner program från Internet eller installera egna program utan tillstånd från IT-funktionen.

IT-konsulter eller medarbetare får inte installera program eller databaser på förbundets arbetsstationer eller servrar utan tillstånd från IT-funktionen.

**Lagringsmedia**

Lagringsmedia (DVD, CD, USB mm) som skapas utanför kontoret kan innehålla virus. Förbundet har ett system som skyddar mot datavirus genom att samtliga filer kontrolleras innan de öppnas. Om systemet upptäcker en smittad fil får du en varning på skärmen och filen öppnas inte. Rapportera detta till IT-funktionen snarast och använd inte smittat lagringsmedia på andra maskiner.

**Molntjänster**

Det finns många olika gratis-tjänster i molnet som kan användas för lagring av information, delning av dokument mm – t.ex. DropBox, GoogleDocs osv. Eftersom dessa tjänster är gratis finns ingen möjlighet att påverka hur information används av de som äger verktygen – information kan lagras utanför EU, personuppgifter kan användas för reklam och det är inte säkert att uppgifter raderas när man stänger sitt konto eller raderar innehåll.

Det finns alltid andra alternativ till dessa tjänster som har godkänts av Datainspektionen och som erbjuder bättre säkerhet. Kontakta IT-funktionen om du har behov av dessa tjänster eller behöver mer information. Självklart får man använda dessa tjänster privat – men aldrig för ST-relaterad information.

**Lagring och säkerhetskopiering av dokument**

ST använder molntjänster för lagring av data – OneDrive, SharePoint mm. Medarbetare har tillgång till lagringsutrymme i molnet och detta får hanteras fritt. Det är leverantören Microsoft som ansvarar för säkerhetskopiering av filerna. Information som lagras i molnet stannar inom EU och används inte för andra syften.

Dokument och andra filer som ska inte lagras på datorn – dessa filer säkerhetskopieras inte.

**Lagring för förtroendevalda**

Tillsammans med mejlfunktionen erbjuder förbundet även en molnlösning för dokumentlagring mm. Även denna tjänst tillhandahålls helt av driftleverantören HPS och är också helt skild från förbundets egna system. HPS ansvara för allt kring tjänsten (behörigheter, konto, support mm).

Förtroendevalda ska inte använda sk gratistjänster för dokumentlagring (GoogleDocs mm) då man inte har någon kontroll över var dokumenten lagras (utanför EU t.ex.) eller säkerheten kring dokumenten. Att lagra dokument hos arbetsgivaren kan vara problematisk vid ev. konflikt och även pga GDPR – om arbetsgivaren inte vill ta ansvar för ev. medlemsinformation som lagras där.

**Avancerad artificiell intelligens**

GPT (Generative Pre-trained Transformer) är en avancerad form av artificiell intelligens vars användning ökar markant i vår omvärld nu och som kan generera text, bilder, musik och andra former av digitalt innehåll. GPT tekniken är en modell tränad på en stor mängd data för att kunna förstå och generera naturligt språk så som modulen ChatGPT. GPT används ofta som ett verktyg för att förbättra produktiviteten och effektiviteten inom många olika områden, men det kan också ha potentiella säkerhetsrisker om det används på ett felaktigt sätt.

ST har ännu inte implementerat denna teknik och erbjuder alltså inte den som en av oss kontrollerad produkt. Därför förbinder du dig som anställd eller förtroendevald att använda GPT endast för icke-känsliga ärenden, att inte dela några personuppgifter eller data genom denna plattform och att du använder de olika GPT modulerna ansvarsfullt och tar ansvar för att skydda informationen och säkerheten för organisationen och våra medlemmar. Du som användare ansvarar också för att faktagranska text eller liknande som kommer ut av användandet av GPT, innan den används.

**Kommunikation**

De allra flesta som har kontakt med ST har det via telefon eller e-post. Vid kontakt ska personen snabbt hamna rätt. Därför är det av yttersta vikt att alla sköter sina kommunikationskanaler på ett bra sätt. Hur vi hanterar telefon, e-post och använder andra kommunikationsmedel påverkar bilden av ST som förbund.

Alla anställda vid ST har en mobiltelefon som är ämnad att kunna lämna arbetsplatsen. Ingen anställd förväntas arbeta utanför normala arbetstider men telefonen är det kommunikationsmedel som ST använder om all personal skulle behöva kontaktas i frågor av akut karaktär.

**Telefon - tillgänglighet och service**

Var och en ansvarar för att den egna anknytningen sköts på ett sätt som gör att ST upplevs som ett förbund med hög servicegrad avseende bemötande och tillgänglighet.

• Svara alltid med ”Välkommen till ST, NN”, med för och efternamn.

• Hänvisa telefonen när du inte är anträffbar.

• Anställda ska lägga in svarsmeddelande i mobilbrevlådan, vilket alltid ska vara ”Välkommen till ST, NN”. Jag kan tyvärr inte svara för tillfället men lämna gärna ett meddelande eller tryck 9 för att komma till telefonist.”

• Ring upp personer som har lämnat meddelande så fort som möjligt.

• Svara så fort som möjligt när det ringer.

**Säkerhet**

Varje förtroendevald/medarbetare är ansvarig för sin användaridentitet och lösenordet. Uppgifterna ska inte läggas synliga vid arbetsplatsen eller spridas till andra**.** Lås datorskärmen när du lämnar din arbetsplats.

Mobiltelefoner och datorer ska alltid förvaras säkert ur stöld- och skadesynpunkt. Dessa kan innehålla känslig information, varför det är av yttersta vikt att de hanteras på ett, i alla avseenden, säkert sätt. Datorer som är kvar på arbetsplatsen efter arbetstid ska förvaras avstängda i låst rum eller skåp. Lämna aldrig värdesaker i parkerad bil.

Användare ansvarar för att förlorad telefon eller dator, utan dröjsmål, anmäls till polisen. Anställda ska också anmäla detta till närmaste chef och IT-support.

**Behörighet**

En säker informationstillgång är avgörande för att genomföra vårt uppdrag. Då information ofta innehåller känsliga uppgifter, såsom medlemskap i fackförening, behöver tillgången till informationen vara genomtänkt för att säkerställa en korrekt hantering. Enligt dataskyddsförordningen är det ett krav att förhindra obehörig tillgång till personuppgifter. Av detta följer kravet på behörighetsstyrning. Det innebär att utöver risker för den enskilde som kan följa av att uppgifter sprids, så finns det även risker för allvarliga och kostsamma konsekvenser för ST om behörigheter och information inte hanteras på ett korrekt sätt. Med behörighet avses tillgång till information i digital form. Detta innefattar information i STs samtliga IT-system.

Vår behörighetshantering ska säkerställa att rätt person har rätt behörighet vid rätt tidpunkt. För att säkerställa en god hanterings ska kansliet och avdelningar/sektioner/klubbar ha mer detaljerade rutinbeskrivningar som kompletterar policyn. Det övergripande syftet är att tydliggöra tilldelning, underhåll och återtagande av behörigheter till och inom system. Den klargör ansvarsfördelningen avseende vem eller vilka som äger rätt att tilldela någon annan, och i så fall vem, behörighet till en viss informationsmängd. Detta gäller medlem, förtroendevalda, kanslianställda och tredje part som har tillgång till STs information.

I ST finns olika uppdrag beskrivna, t ex uppdraget förbundsstyrelseledamot. Även i kansli­organisa­tionen finns uppdrag. Uppdragen skiljer sig åt mellan olika enheter, olika arbetsgrupper inom enheter och ibland mellan olika medarbetartjänster. Ett specifikt uppdrag ska ha en viss behörighet då det gäller tillgång till och möjlighet att ändra eller radera viss information. Med roll avses här den sortering som behövs för att skapa struktur i behörighetshanteringen. Syftet är att ha rätt behörigheter och information i uppdraget. En individ kan ha flera roller i sitt uppdrag. Roll kan, men behöver inte, vara likställt med en titel eller en organisatorisk funktion. Exempel på roll är förbunds­ordförande, rådgivare eller ombudsman.

Behörighetsgrupp avser en eller flera behörigheter som en eller flera roller har gemensamt. Bland behörighetsgrupperna finns förtroendevald, kanslianställd och tredje part.

* Med förtroendevald avses medlem som valts till ett förtroendeuppdrag i ST.
* Med kanslianställd avses personer som är anställda av ST eller konsult som ersätter anställd
* Med tredje part avses t ex auktoriserade revisorer eller konsulter från en leverantör.

### Grunden för behörighetstilldelning

För att informationstillgången ska vara säker är utgångspunkten att behörigheter följer uppdraget. Förtroendevalda och medarbetare får då tillgång till den information som behövs för att genomföra sina uppgifter. Informationstillgång är del i verksamhetsstyrningen, en god intern kontrollmiljö och bidrar till efterlevnad av interna rutiner och lagkrav.

Grunden för behörighetstilldelning och återtagande är:

* Tilldelning av behörigheter ska motiveras av medlems- och verksamhetsnytta.
* Beslut om tillgång till information ska fattas enligt nedan beskrivet ansvar för behörigheter. Tillgång ska även ta hänsyn till skyddsnivå avseende grad av känslighet och informationsmängd.
* Alla ska ges tillgång endast till den information som behövs för att fullgöra sitt uppdrag och arbete enligt etablerade arbetssätt och system. Genom att matcha rollens ansvar med tilldelad be­hörig­het skyddas individen som utför uppdraget genom att risken för felhantering begränsas. För att värna registrerades integritet ska behörigheter minimeras till vad som är nödvändigt för att utföra uppdraget.
* För att säkerställa kvaliteten på STs information ska endast behöriga personer ha rätt att skapa, ändra eller radera information. Loggning ska ske för att kunna spåra förändringar av informationen som gjorts. Behöver personen inte skapa, ändra eller radera information i sin roll ska behörigheten vara titta-behörighet, dvs. att endast kunna läsa informationen.

### Ansvar för IT-lösningar och behörigheter

Förbundsstyrelsen är ytterst ansvarig för STs informationssäkerhet. Förbundsstyrelsen ansvarar och beslutar om övergripande policy samt riktlinjer och tillgång till IT-lösningar för förtroendevalda.   
  
Kanslichefen ansvarar för kansliets IT-lösningar samt beslutar om behörigheter som gäller kansliets medarbetare och tredje part. Verkställande och beslut kan delegeras till kansliets chefer.

Ovarsam användning av IT-resurserna eller underlåtenhet att följa reglerna kan leda till förlust av rätten att använda IT-resurserna, till disciplinära och/eller rättsliga påföljder.

**Bilaga 1**

**Rutiner för abonnemang, användning och administration**

Mobilabonnemanget är ett företagsabonnemang som är knutet till användaren. Mobiltelefonen ägs av ST.

**Beställning**

Beställning av datorer, mobiltelefoner, tillbehör och abonnemang sköts av IT. Enhetschefen tillser att beställning initieras. Chefen ansvarar också att eventuella förändringar meddelas till IT-enheten.

Chefen säkerställer att uppgifter om förändringar, eller nya uppgifter, skickas till IT-enheten i god tid. Chefen säkerställer att varje anställd som skall ha en dator eller telefon får abonnemang och utrustning genom IT-funktionen.

Chefen ansvarar för attest av mobiltelefonräkningar inom sin enhet.

**Användares frånvaro från arbetsplatsen**

Vid föräldraledighet eller längre frånvaro (ej tjänstledighet för att prova annat arbete) har medarbetaren rätt att behålla sin mobiltelefon. ST står då för abonnemanget och den anställde står för samtalskostnaderna.

**Uppsägning av mobilabonnemang**

Uppsägning av mobilabonnemang görs till IT-enheten.

**Reparation**

Vid trasig telefon gäller följande: Telefon lämnas till IT för bedömning av åtgärd. Under reparation erbjuds den anställde en lånetelefon.

### Bilaga 2

Av kansliet framtagna rutiner som kompletterar behörighetspolicyn med mer detaljerad rutinbeskrivning av behörighetshanteringen som beslutas av ledningsgruppen.

Behörighetsrutiner för IT-system

Beslutad av ledningsgruppen 2020-09-14

### Bakgrund

Fackförbundet ST har en mängd olika IT-system som används av olika medarbetare vid olika tillfällen. Våra behörighetsrutiner är till för att säkerställa att rätt medarbetare har rätt behörighet vid rätt tidpunkt utifrån den av förbundsstyrelsen beslutade behörighetspolicyn.

I systemförteckningen som länkas till sist i dokumentet framgår vilka system ST använder sig av, vem som är ansvarig respektive förvaltare, systemtyp samt om systemet är aktivt. Förteckningen ska hållas uppdaterad av ansvarig på IT.

### Allmän behörighet

ST använder ett centralt register för hantering av samtliga konton – ett s.k. Active Directory (AD). För att överhuvudtaget får tillgång till STs IT-miljö måste en användare har ett konto i AD-et. Alla medarbetare på ST har ett konto i AD-et som bl.a. ger tillgång till Office programmen och lagringsutrymme i molnet.

Sedan tillkommer ett antal andra system (medlemsregistret (CRM), tidrapportering (AGDA), fakturor (Hogia) m.fl. Åtkomst till dessa system ges när en medarbetare har loggat in med sitt AD-konto. Vissa av dessa system kan man sedan komma in direkt i (Agda, CRM) medan andra kräver ytterligare en inloggning (Hogia). Målet är att samtliga system ska kunna nås direkt när man har loggat in med sitt AD-konto men olika leverantörer har olika tidplan för detta. Se nedan bilaga 1 för vilka system ST använder och har information lagrad i.

Behörigheter är kopplade till medarbetarens roll – är man ombudsman har man tillgång till vissa system, är man rådgivare till andra.

### När skapas ett AD-konto?

Information om att en medarbetare har anställts kommer från HR via ett arbetsflöde. HR skapar ett dokument med uppgifter om medarbetaren (namn, roll, startdatum osv.) och dokumentet skickas automatiskt till bl.a. IT.

Kontot skapas i AD-et så fort IT får information om att en medarbetare ska börja – men kontot är inaktiverat vilket betyder att det inte kan används och syns inte i någon adresslista. Utifrån medarbetarens roll tilldelas nödvändiga behörigheter.

En månad innan medarbetaren börjar görs kontot aktivt – den syns i adresslistor och kan ta emot mejl och kalenderbokningar. För chefer kan detta ske upp till tre månader innan anställningen påbörjas.

När medarbetaren hämtar sin utrustning på kansliet lämnas kontouppgifterna ut. För anställda som börjar på lokalkontoren skickas kontouppgifterna till den som ska ta emot den nya medarbetaren. Lösenordet måste bytas vid första inloggningen.

### Ansvar för tilldelning och återtagande av behörigheter

Behörighetshantering ska vara så automatiserad som möjligt och behörigheterna ska därför tilldelas från definierade roller i medlemssystem och register med anställda. Den som registrerar en tilldelad roll i systemet initierar därmed också behörighetshanteringen.

Systemägare ansvarar för att respektive IT-system har en strukturerad och dokumenterad behörighetshantering.

Systemägaren ska göra en årlig översyn av behörigheter så att tidigare behörigheter inte felaktigt ligger kvar då uppdrag eller anställning upphört eller förändrats. Ansvarig för kontroll att så sker är verksamhetscontrollern.

Systemförvaltaren ansvarar för den konkreta behörighetshanteringen i systemet.

Behörighet tilldelas utifrån roll för rationell hantering och förenklad dokumentation. Behörighets­struk­turen blir förutsägbar och enhetlig.

Behörigheter kan tilldelas i olika nivåer och ge olika rättigheter. Behörighet i ett IT-system tilldelas på olika nivåer t ex administratör, användare osv. och ger olika rättigheter som att läsa, skapa, ändra, radera eller distribuera vidare information.

Alla som tilldelats en behörighet ska vara uppmärksamma på vilka behörigheter de har och rapportera till närmaste chef om de har tillgång till mer eller mindre information än de behöver för att fullfölja sitt uppdrag.

Avsteg kräver medvetna beslut som dokumenteras för spårbarhet och som löpande följs upp och omprövas av systemägaren. Avsteg från beslutad behörighetshantering ska vara tidsbestämda och gälla högst ett år.

### Ändring av behörigheter

Om en medarbetare behöver tillgång till andra system, utökade behörigheter osv. är det den närmaste chefen som måste godkänna detta och informera IT i förväg. Information om att medarbetarens behörigheter har ändrats skickas via mejl till medarbetaren och medarbetarens chef.

### När stängs ett konto?

HR informerar IT om en medarbetare ska sluta. IT kontaktar medarbetaren direkt och informerar om att medarbetarens konto kommer att avaktiveras sista arbetsdagen vilket betyder att den inte längre kan användas.

IT informerar medarbetarens närmaste chef om att – om inget annat begärs –kontot kommer att raderas helt efter en vecka. All information tas då bort.

Om en medarbetare är tjänstledig (gäller ej föräldralediga) avaktiveras kontot och kan inte användas. HR informerar IT när medarbetaren ska återkomma, alternativt slutar.

Särskild överenskommelse kan träffas med den tjänstledige om att bibehålla kontot under en period efter påbörjad tjänstledighet/avslut för att färdigställa specifika uppgifter.

Om en medarbetare är föräldraledig lämnas kontot oförändrad då de flesta vill ha kontakt med arbetet under ledigheten. Om en medarbetare efter diskussion med sin chef vill inte ha åtkomst till sitt konto under ledigheten avaktiveras kontot och aktiveras först när medarbetaren åter är i tjänst.