It-policy

Det här dokumentet beskriver regler och riktlinjer för användningen av it-resurser inom Polarforskningssekretariatet. Med it-resurser menas datorer, nätverk, system och all annan kringutrustning som används i samband med hantering av information i digital form.

Reglerna gäller alla anställda och samtliga övriga användare av myndighetens it-resurser som till exempel praktikanter och externa konsulter. Avsikten med dokumentet är att skydda myndighetens verksamhet och anställda. Denna policy kommer att bli föremål för tillägg och förändringar när så krävs.

Grundläggande princip

Den grundläggande princip på vilken dessa regler och riktlinjer vilar, är att myndighetens it-resurser ägs av myndigheten och utgör ett arbetsredskap som ska användas för myndighetens verksamhet. Myndigheten ska inte lida skada eller onödiga kostnader genom olämplig användning av dessa arbetsredskap.

Myndighetens it-resurser ska användas med gott omdöme och får inte användas för att på otillbörligt sätt sprida, förvara eller förmedla information

- i strid mot gällande lagstiftning om till exempel behandling av personuppgifter, hets mot folkgrupp, barnpornografibrott, olaga våldsskildring, förtal, ofredande, dataintrång eller upphovsrättsbrott
- som är att betrakta som politisk, ideologisk eller religiös propaganda
- som i annat fall kan uppfattas som kränkande och stötande
- som syftar till att marknadsföra produkter eller tjänster
- som på något annat sätt kan störa myndighetens it-verksamhet.

Myndigheten ansvarar för att introduktionen av nyanställd personal omfattar it-policy och it-säkerhet. Därutöver ska kunskapen hos all personal uppdateras årligen med utbildning om informationssäkerhet.

Individuellt ansvar

Det är viktigt att alla berörda inser det individuella ansvar som denna policy innebär. Som användare förväntas du känna till och följa dessa regler och riktlinjer. Det är också viktigt att användandet av myndighetens it-resurser görs på sådant sätt att myndighetens namn, anseende och goda rykte bibehålls.

Behörighet

Behörigheten till myndighetens it-resurser är personlig och får inte överlåtas eller på annat sätt göras tillgänglig för annan anställd eller extern part. Det är inte tillåtet att nyttja någon annans behörighet eller utnyttja felaktiga konfigurationer, programfel eller på annat sätt manipulera myndighetens it-resurser.

Grundläggande av behörigheter tilldelas av närmsta chef och ska så långt det är möjligt vara rollbaserad och/eller styras på behörighetsgruppnivå. Tillgången till verksamhetssystem stäms av med respektive systemansvarig. Varje it-system ska ha en ansvarig som tilldelar och regelbundet reviderar behörigheter i systemet. Denna revision ska ske minst en gång per år. Vid förändring av arbetsuppgifter eller till- och frånträde från tjänst ska översyn och uppdatering av behörigheter ske omedelbart.

Grundregeln är att all information lagrad i myndighetens gemensamma struktur är tillgänglig internt för alla. Undantag utgörs av personuppgifter och andra känsliga uppgifter inom HR-området där behörighet endast ska tilldelas HR-ansvarig och administrativ chef. Behörighet till hälsoundersökningar vid expedition tilldelas endast medicinsk personal. Särskilda behörighetsgrupper ska också gälla för mätdata från observationer och miljöövervakning i Abisko samt motsvarande forsknings- och annan mätdata på Oden.

Endast it-ansvarig ska ha tillgång till övervakning och loggar kopplat till det lokala nätverket.

Säkerhet

Användaren är ansvarig för att upprätthålla informationssäkerheten genom att följa beslutade rutiner och använda it-miljön på ett sådant sätt att de tekniska säkerhetslösningarna inte åsidosätts eller kringgås.

För att skydda mot spridning av virus och mot obehörigt tillträde skyddas våra it-resurser av säkerhetssystem, såsom skräppostfilter, antivirusskydd och brandväggar. Det är inte tillåtet att avaktivera eller på något sätt manipulera dessa skydd.

Alla anslutningar och installationer av datorer eller annan utrustning i myndighetens nätverk ska utan undantag godkännas av it-ansvarig.

Användaren är ansvarig för en säker användning av sin personliga utrustning och att vidta alla rimliga åtgärder för att skydda it-resurser mot virus, obehörigt tillträde eller andra attacker mot systemets säkerhet och integritet.

Vid inloggning med lösenord ska användaren försäkra sig om att ingen annan kan se vilket lösenord som matas in. När användaren lämnar datorn utan tillsyn ska obehörig

tillgång till datorn förhindras genom att s k skärmlås aktiveras så att lösenord måste anges för upplåsning. Som ett komplement för att minska risken vid glömska eller oaktsamhet ska automatisk utloggning eller automatisk skärmlåsning användas.

Lösenord och användaridentitet

Varje individ som ska beredas tillgång till Polarforskningssekretariatets nätverk ska identifieras med en personlig användaridentitet som lagras i myndighetens centrala autentiseringssystem.

Lösenord och användaridentitet ska ses som personliga uppgifter och ska hanteras med varsamhet och får inte lämnas ut till någon annan. Användaren är ansvarig för att obehöriga inte får tillgång till det personliga lösenordet. Lösenord ska av användaren omgående bytas om misstanke finns att det har avslöjats. It-ansvarig förbehåller sig rätten att omedelbart byta en användares lösenord vid misstanke om att lösenordet avslöjats.

Användare får inte använda samma lösenord till externa system eller för privat bruk (till exempel Facebook och Gmail) som till myndighetens resurser.

Lösenordet ska uppfylla de krav på komplexitet som myndigheten vid varje tidpunkt bedömer vara nödvändigt enligt gällande anvisningar (för närvarande minst 8 tecken långt, minst en gemen, versal, siffra eller annat tecken) och ska bytas ut minst var 6:e månad (tvingande funktion).

Internet

Internet är avsett att användas för informationssökning och andra relevanta ändamål inom och för myndighetens verksamhet.

Vid användning av internet är det till exempel förbjudet

- att besöka webbsidor med pornografiskt eller extremistiskt innehåll
- att ladda ner program och filer om de kan påverka it-säkerheten på myndigheten, vid osäkerhet kontakta it-ansvarig
- att sprida eller förfoga över upphovsrättsligt skyddat material utan rättighetsinnehavarens tillstånd
- att besöka spelsidor, spela förströelsespel eller liknande.

E-post

E-post är avsedd att användas för intern och extern kommunikation. All e-postkommunikation som avser myndighetens verksamhet ska ske genom myndighetens

e-postkonton där det klart ska framgå för mottagaren att mejlet kommer från myndigheten.

Användare får inte använda myndighetsadressen på ett sätt eller i ett sammanhang som kan skada myndighetens anseende. E-post får inte användas för politiska, kommersiella eller andra syften som strider mot myndighetens verksamhet. E-posten får inte användas för privat bruk, användas i privata diskussionsgrupper, som mottagaradress för privat reklam eller på andra sätt som kan skada myndigheten.

Mobiltelefon och bärbar dator

Det är av yttersta vikt att den anställde hanterar sin mobiltelefon och bärbara dator med största varsamhet och försiktighet med tanke på vilken säkerhetsrisk denna typ av utrustning innebär.

Programvaror

I första hand ska standardprogram användas för att tillgodose användarnas behov. Användare får inte installera annan programvara utan godkännande av it-ansvarig.

Privat användning av it-resurser

Användare har fått tillgång till it-resurser för att underlätta deras arbete för myndigheten och resurserna får inte missbrukas. Emellertid är privat användning acceptabelt under förutsättning att

- användningen inte stör några direkta eller indirekta åtaganden med eller för myndigheten
- användningen inte medför några kostnader för myndigheten
- användningen följer reglerna i denna policy.

Fjärråtkomst

Myndigheten tillhandahåller säker fjärråtkomst till sina it-resurser för de medarbetare som har det behovet. Det åligger användaren att säkerställa att de datorer som används för fjärråtkomst lever upp till de krav som ställs för god it-säkerhet (avseende antivirus, personlig brandvägg med mera). Vid osäkerhet om så är fallet ska användaren först stämma av detta med it-ansvarig.

Kontroll och övervakning av it-system

Användare som vid användande av myndighetens it-resurser upptäcker fel eller annat som kan vara av betydelse för it-driften inom myndigheten, är skyldig att genast

rapportera detta till närmsta chef eller it-ansvarig. Myndighetens rutiner för incidentrapportering och personuppgiftsincidenter ska tillämpas.

It-resurserna övervakas kontinuerligt och händelser på det lokala nätverket loggas. Dessa loggar sparas och arkiveras och kan vid behov utgöra bevis för eventuella överträdelser.

Information i myndighetens it-system kan komma att kontrolleras.

Överträdelser

Överträdelser mot denna it-policy kan leda till disciplinära påföljder och vid allvarliga överträdelser uppsägning. Olagliga handlingar kommer att polisanmälas.

Informationsklassning

Myndigheten ska vid klassning av information utgå från den modell som tagits fram av Myndigheten för samhällsskydd och beredskap (MSB). Informationstillgången värderas inom varje säkerhetsaspekt konfidentialitet, riktighet och tillgänglighet och anpassas och konkretiseras till organisationens verksamhet.