VARA KOMMUN

Riktlinjer

IT-säkerhet för användare

Antagen av kommundirektören 2013-12-01

Innehållsförteckning

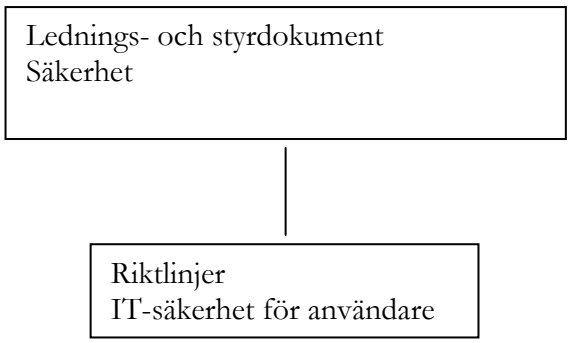
Bakgrund 1
Riktlinjens roll i IT-säkerhetsarbetet 1
Inledning 1
Omfattning 1
Allmän skyldighet 1
Särskilda regler för vissa system 2
Miljöansvar 2
Arbetsplatsen 2
Identitetskrav vid IT-hjälp 2
Inköp och anslutning av dator eller kringsutrustning 2
Icke fungerande IT-utrustning 2
Programinstallation 2
När medarbetaren lämnar arbetsplatsen 3
Utskrifter 3
Fjärrstyrning 3
Arbeta hemifrån 3
Programkopiering 3
Behörighet 3
Grundbehörighet 3
Utökade behörigheter 4
Lösenord 4
Inloggning 4
Tillfälligt utökade rättigheter 4
Ansvar 5
Upplåsning av användarkonto eller e-postkonto 5
Byte av arbetsuppgifter/avslutande av anställning 5
Lagring av information 5
Hemkatalog 5
Verksamhetsgemensam 5
Samverkan 5
Lagringsutrymme 6
Bärbara datorer, mobila enheter och USB-minnen 6
Skrivare 6
Nätverksskrivare 6
Lokala skrivare 7
Internet 7
Internetanvändande generellt 7
Material från internet 7
Strömmande media 7
E-post 7
Virusskydd 8
Incidenthantering 8
Sanktioner vid regelbrott 8

Bakgrund

Riktlinjens roll i IT-säkerhetsarbetet

IT-säkerhet är en del i kommunens lednings- och kvalitetsprocess som ska bidra till att ett IT-system kan användas på avsett sätt och med avsedd funktionalitet. Myndigheten för samhällsskydd och beredskap (MSB) rekommendationer om basnivå för IT-säkerhet ska gälla som ramverk för IT-säkerhetsarbetet.

Styrande dokument för IT-säkerhetsarbetet är *lednings- och styrdokumentet rörande säkerhet* och r*iktlinjer för IT-säkerhet för användare.* Riktlinjerna rörande IT-säkerhet är en konkretisering av lednings- och styrdokumentet rörande IT. Krav på och åtgärder för ett enskilt IT-system ska dokumenteras i en *system-säkerhetsplan*. En sådan ska upprättas för de IT-system som bedöms som viktiga för verksamheten.



Lednings- och styrdokumentet rörande säkerhet redovisar kommunens viljeinriktning och mål för säkerhetsarbetet. I styrdokumentet för säkerhet ingår IT-säkerhet som en naturlig del.

Riktlinjer - IT-säkerhet för användare (detta dokument) syftar till att ge de anställda kunskaper och riktlinjer om hur man på ett säkert sätt använder IT-stöden.

Inledning

Riktlinjen berör alla som är användare av kommunens IT-verktyg.

Omfattning

Dessa säkerhetsriktlinjer avser alla kommunanställda som är användare. Av praktiska skäl finns ibland mindre skillnader i regelverket beroende på verksamhet. Där det förekommer anges detta särskilt.

Riktlinjerna används i tillämpliga delar för skolans elever.

Allmän skyldighet

Information är en mycket viktig tillgång för vår kommun. För att skydda de värden informationen representerar krävs ett säkerhetsmedvetande hos alla medarbetare. Användarna har alltså en stor del av ansvaret för säkerheten i

informationshanteringen. För att kunna leva upp till de säkerhetskrav som ställs, är alla medarbetare skyldiga att känna till:

- vilka regler som gäller och vilket ansvar som varje medarbetare har
- vad medarbetarna ska göra i olika situationer
- var medarbetarna kan få stöd och hjälp

Användaren kan alltid vända sig till IT-servicedesk för hjälp och stöd.

Särskilda regler för vissa system

Observera att vissa system, som hanterar särskilt känsliga uppgifter, kan ha striktare säkerhetsregler än de som beskrivs här. Om något av de system användaren använder innehåller särskilt känsliga uppgifter bör användaren därför kontrollera med systemansvarig om det finns kompletterande säkerhetsriktlinjer för det systemet.

Aktuell lista över systemansvariga finns på Insidan (kommunens intranät).

Miljöansvar

Användaren ansvarar för att stänga av eller aktivera viloläge när datorn inte används för att inte använda onödig energi. Användaren ansvarar även för att datorutrustning inte slängs bland vanligt avfall utan går via IT-avdelningen till återvinning.

Arbetsplatsen

Identitetskrav vid IT-hjälp

IT-avdelningens personal finns dokumenterad på Insidan med namn och foto.

Inköp och anslutning av dator eller kringsutrustning

All IT-utrustning ska beställas genom IT-avdelningen. All installation och konfiguration av arbetsstationer och annan kringutrustning ska ske av IT-avdelningen, för att säkerställa att organisationens standarder följs och IT-säkerheten upprätthålls. Även flytt av dator ska anmälas till IT-servicedesk, som då tillser eventuella säkerhetsmässiga förändringar. Utrustning som inte godkänts via IT-avdelningen får av säkerhetsskäl inte kopplas in i vårat nätverk.

Icke fungerande IT-utrustning

Om dator, annan IT-utrustning eller IT-relaterad utrustning inte fungerar, ska IT-servicedesk kontaktas.

Programinstallation

Program som godkänts av IT-enheten finns för hämtning till datorn under självbetjäningsportalen (IT-servicedesk kan även kontaktas för support).

Finns behov av annan programvara ska IT-enheten kontaktas för nytt upplägg i självbetjäningsportalen.

Övrig programvara som inte godkänts av IT-avdelningen får inte installeras eller användas på arbetsstationer eller i nätverk som administreras av

organisationen. Naturligtvis gäller detta även program som kan anskaffas från internet.

I vissa verksamheter kan det finnas behov av att ladda ner tillfällig programvara över internet (exempelvis inom skolverksamheter). Det får då bara handla om programvara som fritt får nyttjas och inte kräver någon form av licens. Naturligtvis ska upphovsrättsliga lagar följas i vår organisation, d.v.s. ingen nedladdning av upphovsrättsskyddad programvara får ske. Backup, ominstallation, avinstallation eller dylikt som rör denna mjukvara ombesörjes av användaren. IT-avdelningen förbehåller sig rätten att avinstallera dylika program om de kan antas orsaka andra fel på datorn eller i nätet.

När medarbetaren lämnar arbetsplatsen

När en medarbetare lämnar arbetsplatsen ska denne använda skärmsläckare med lösenordsskydd, alternativt logga ut, även om det bara är för en kortare stund.

Utskrifter

Utskrifter av dokument på en gemensam skrivare ska hämtas så snart som möjligt.

Fjärrstyrning

För att lösa vissa datorproblem kan IT-avdelningen behöva ta över och fjärrstyra en dator. Detta får bara ske om användaren godkänt denna åtgärd. När användaren inte är inloggad har dock IT-avdelningen rätt att, utan godkännande, fjärrstyra datorn i samband med nödvändigt tekniskt underhåll.

Arbeta hemifrån

Närmaste chef avgör om en medarbetare har rätt att arbeta hemifrån. Distansanslutning finns som IT-tilläggstjänst. Tänk på att riktlinjer för IT-verktygen även gäller vid arbete hemifrån.

Programkopiering

Det är inte tillåtet att kopiera eller använda kommunens program utanför organisationens verksamhet.

Behörighet

Vara kommuns nätverk är utrustade med ett behörighetskontrollsystem (BKS) för att säkerställa att det bara är behöriga användare som kommer åt information och att en användare enbart kan komma åt den information som den behöver för att utföra sina arbetsuppgifter. Identiteterna i vårt BKS bygger på de tilltalsnamn och de stavningar av namn som finns registrerade hos skattemyndigheten.

Grundbehörighet

Vid anställning förs den anställde in i Vara kommuns personalhanteringssystem som i sin tur styr den anställdes grundbehörigheter. Tillsvidare och visstids-anställda får per automatik användar-ID och e-post. För timanställda får berörd chef ansöka om användar-ID och e-post. Ytterligare information för chefer kan fås i speciella riktlinjer för användarhantering.

Utökade behörigheter

Utökade behörigheter för verksamhetssystem ansöks av den anställdes chef och tilldelas av respektive systemansvarig.

Utökade filrättigheter ansöks via självbetjäningsportal, där mappägaren ansvarar för behörighetskontrollen.

Lösenord

Samma inloggning som du använder till inloggningen använder du även till e-postsystemet.

Första gången du ska logga in blir du tilldelad ett användar-ID och ett tillfälligt lösenord av din chef. Detta lösenord måste bytas till ett eget lösenord vid första inloggningstillfället.

För personal gäller (om chefen inte meddelar annat) att lösenordet måste bestå av minst 10 tecken, varav minst en siffra, minst en stor bokstav och minst en liten bokstav (elever minst 8 tecken med samma regler om siffror och bokstäver) Lösenordet ska inte innehålla å, ä, ö eller andra bokstäver som inte finns i engelska alfabetet. Lösenordsreglerna hindrar att använda lösenord som innehåller användarens för- efternamn, användar-ID eller födelsedata.

Lösenord är personliga, vilket innebär att användare inte får avslöja lösenordet för någon annan eller låna ut sin behörighet. Lösenordet ska vidare skyddas väl och ska bytas omedelbart om lösenordet avslöjats. Undvik att dokumentera lösenord på papper om det inte kan förvaras helt säkert.

Ändra lösenordet regelbundet. Efter 90 dagar kräver behörighetssystemet att du byter ditt lösenord (elever 180 dagar). Meddelande på skärmen visas med början 14 dagar före sista möjliga byte. Om byte inte sker låses kontot. Endast IT-servicedesk kan då låsa upp kontot.

Har du koppling till användar-ID på andra enheter, t.ex. telefon med automatisk tillgång till e-post och kalender måste du även byta lösenordet till detta efter byte på datorn.

Om du glömmer ditt lösenord för inloggning i nätverket ska du kontakta IT-servicedesk för att få ett nytt tillfälligt lösenord.

Du kan även av din chef få användar-ID och lösenord som gäller till specifika verksamhetssystem. Glömmer du lösenordet till något av dessa system ska du kontakta systemansvarig för respektive system.

Inloggning

Det är inte tillåtet att logga in eller försöka logga in med annans identitet.

Det är inte heller tillåtet att låta utomstående, (t.ex. barn, nära anhörig, försäljare) använda användarens dator eller dennes inloggning.

Tillfälligt utökade rättigheter

Genom ansökan i självbetjäningsportalen kan utökade rättigheter fås för t.ex. installation av skrivare på distansarbetsplats.

Ansvar

All hantering inom befintliga system loggas, vilket bl.a. har till syfte att kunna spåra obehöriga intrång. Detta innebär att användaren är ansvarig för allt som registreras med användaridentiteten. När en medarbetare lämnar arbetsplatsen ska denne använda skärmsläckare med lösenordsskydd, alternativt logga ut, även om det bara är för en kortare stund.

Upplåsning av användarkonto eller e-postkonto

Skulle upplåsning av användarkonto eller e-postkonto vara nödvändigt på grund av användarens ledighet, sjukskrivning eller annan frånvaro, krävs skriftligt godkännande från användarens chefs närmaste chef.

Byte av arbetsuppgifter/avslutande av anställning

Den anställde ansvarar för att rensa hemkatalog och e-post vid avslutad tjänst.

Vid behov ska närmaste chef rådfrågas. Närmaste chef bestämmer sedan hur de dokument m.m. som ska sparas ska hanteras. Respektive chef ansvarar för avanmälan för de utökade rättigheter som den anställde haft i respektive verksamhetssystem.

Automatisk inaktivering av konto sker efter avslutad anställning och styrs av kommunens personalhanteringssystem.

Vid byte av tjänst kommer rättigheter förändras utefter ändrade uppgifter i personalhanteringssystemet.

Lagring av information

Inom kommunen hanteras material av stor betydelse. Det är därför viktigt att alla hanterar material på ett säkert sätt.

Det tillgängliga utrymmet i kommunens servrar som används till att lagra dokument och e-post är mycket begränsat. För att detta utrymme ska räcka till för alla måste det finnas ett tak för hur mycket utrymme varje användare kan förbruka.

Den information du lagrar på nätverket säkerhetskopieras automatiskt. Du ska därför lagra din information i verksamhetsgemensam, samverkan eller i din hemkatalog.

Hemkatalog

Egen hemkatalog är ditt personliga arkiv som du ska använda för lagring av personligt arbetsmaterial. Filerna kan endast nås genom din personliga inloggning.

Verksamhetsgemensam

Verksamhetsgemensam är ett arkiv för lagring av information som alla inom din verksamhet har tillgång till.

Samverkan

Samverkan är ett arkiv för lagring av information mellan olika grupper.

Tänk på att det som lagras lokalt på din dator är tillgängligt för alla som kan starta din dator. Man behöver oftast inte använda något lösenord för att komma åt information på datorn. Om du lagrar information på din lokala dator eller externt lagringsmedia, till exempel USB-minne så är du personligen ansvarig för att informationen blir säkerhetskopierad. När du lagrar information på din dator riskerar du att förlora information som inte kan återskapas till rimliga kostnader. Du försvårar också för dina medarbetare att ta del av informationen.

Du är ansvarig för att den information du skapar hanteras på rätt sätt. Om du arbetar med känslig och sekretessbelagd information ska du få information från din chef om hur denna hanteras. Du ska i samband med denna information skriva under en förbindelse om sekretess och tystnadsplikt.

Lagringsutrymme

Varje användare har ett begränsat lagringsutrymme för personliga filer samt e-post. Personliga filer och epost ska användaren regelbundet gå igenom och städa. Personligt lagringsutrymme är begränsat till 2GB per användare för filer samt 500Mb för e-post. Vid behov av utökat lagringsutrymme kontaktar du din chef som i sin tur gör en beställning vid behov.

Bärbara datorer, mobila enheter och USB-minnen

Bärbara datorer, plattor och USB-minnen ska låsas in eller hållas under uppsikt.

Angående lagring se ”Lagring av information” ovan.

För den som handskas med känslig eller sekretessbelagd information räcker inte inloggningslösenord som säkerhet. På bärbara medier, så som bärbara datorer, plattor och USB-minnen, ska ytterligare skydd då användas, (t.ex. kryptering, extra koder). Instruktioner ges av IT-avdelningen.

De bärbara datorerna ska regelbundet anslutas till nätverket så att de får ta del av nödvändiga säkerhetsuppdateringar och får uppdateringar till sitt antivirusprogram.

Skrivare

Det finns två olika typer av skrivare:

- Nätverksskrivare
- Lokala skrivare

Nätverksskrivare används i första hand då dessa oftast har en lägre driftskostnad.

Nätverksskrivare

I kommunens nätverk finns ett antal nätverksskrivare där användarna själva har möjlighet att ansluta sig.

Lokala skrivare

Lokal (personlig) skrivare kan erhållas om användaren t.ex. hanterar mycket sekretessmaterial eller mycket skrymmande mängder material. För erhållande av egen skrivare krävs närmaste chefs godkännande.

Internet

Kommunens nätverk är anslutet till internet via brandväggar som reglerar in och utgående trafik. I brandväggarna sker också en registrering av vilka sidor som besöks. Allt användaren gör på Internet loggas och loggarna sparas. När en medarbetare surfar på internet representerar denne kommunen. Det är därför viktigt att alla agerar i enlighet med kommunens regler och riktlinjer så att det som förmedlas genom internetanvändningen inte skadar kommunen.

Internetanvändande generellt

Under arbetstid får endast för arbetet relevanta webbsidor besökas. Det är inte tillåtet att använda kommunens internetuppkoppling eller datorer för att surfa på olagliga eller på annat sätt kränkande eller anstötliga sidor. Om så sker kommer det att polisanmälas och eventuella arbetsrättsliga åtgärder att vidtas. Det är inte tillåtet att via internet titta eller lyssna på material av pornografisk eller rasistisk karaktär. Förbudet gäller också material som är diskriminerande (religion, kön, sexuell läggning etc.) eller har anknytning till kriminell verksamhet.

Material från internet

Naturligtvis ska upphovsrättsliga lagar följas i vår organisation, d.v.s. ingen nedladdning av upphovsrättsskyddat material får ske. Du får endast ladda hem filer som är relevanta för dina arbetsuppgifter.

Strömmande media

Strömmande media, såsom exempelvis webbradio, musik, TV och film, tar mycket kapacitet från vår internetförbindelse. Av hänsyn till andra användare är det därför extra viktigt att undvika denna typ av internetanvändning, annat än när detta behövs för att utföra sina arbetsuppgifter.

E-post

E-post är ett redskap som i första hand ska användas i tjänsten. Tänk på att all e-post är allmän handling så fort den kommit in i brevlådan. E-post ska behandlas och diarieföras på samma sätt som övrig post. Om du är frånvarande ska du sätta frånvarobesked med uppgift om vem som hanterar dina ärenden och ge någon annan fullmakt att sköta brevlådan.

Sekretesshandlingar eller känsliga handlingar får inte skickas som e-post.

E-post med bilagor utgör ett stort hot när det gäller spridning av virus. För att undvika risk för virusspridning bör du vara försiktig med bifogade filer. Öppna endast filer du känner till och från avsändare du litar på.

Du bör vara återhållsam med att använda stora gruppadresser (massutskick) och med att skicka eller vidarebefordra meddelanden som innehåller stora filer. Du bör inte heller skicka eller vidarebefordra kedjebrev av någon sort.

Det är inte tillåtet med automatisk vidarekoppling till adresser utanför kommunen.

För att förhindra mängden skräppost (spam) i våra e-brevlådor finns ett skräppost-filter installerat på vår e-postserver. För att minska risken för skräppost ska du inte lämna ut din e-postadress till webbplatser som du inte uppfattar som seriösa.

Använd inte din vanliga användaridentitet och ditt lösenord när du registrerar dig i kundregister eller publika e-postservrar.

Om du får hotelsebrev eller liknande ska du kontakta din chef.

Det är inte heller tillåtet att synkronisera privata enheter mot kommunens e-post. Måste en privat enhet användas så ska komunens epostportal användas (epost.vara.se).

Virusskydd

Alla kommunens datorer ska innehålla uppdaterat virusskydd, vilket inte får avaktiveras. Datorn ska även vara uppdaterad med operativsystemets senaste säkerhetsuppdateringar.

Datavirus kan beskrivas som ett program eller en programsekvens vars uppgift är att kopiera sig själv och tränga in i andra program för att utföra något otillbörligt. I bästa fall är det oskyldiga pip eller hälsningar som ritas på skärmen. I värsta fall raderas datorns hårddisk eller så kopierar viruset sig självt i det oändliga tills hela systemet bryter samman. Väl inne i nätverket kan det sedan sprida sig vidare till andra datorer. Datavirus är ofta ytterst smittsamma och ”smittkällan” kan ibland vara svår att identifiera. Oftast sprids de via olika program och filer som laddas ned från internet t.ex. via chat och e-post.

Incidenthantering

Vid misstanke om att någon obehörig använt en medarbetares användar-identitet och varit inne i systemet ska närmaste chef och IT-avdelningen kontaktas.

Vid misstanke om datavirus ska närmaste chef och IT-avdelningen kontaktas.

Vid misstanke om stöld, brand, sabotage eller dylikt ska närmaste chef och IT-avdelningen kontaktas, efter kontakt med 112 eller 114 14.

Sanktioner vid regelbrott

Användare som bryter mot dessa riktlinjer riskerar få en skriftlig varning. Åtföljs ändå inte riktlinjerna kan det medföra arbetsrättsliga åtgärder. Lagbrott medför polisanmälan.

……
Kommundirektör, Gert Norell