SURAHAMMARS KOMMUN

Surahammar 2019-10-04

Användarinstruktion

För Surahammars kommuns datorer och nätverk

Inledning

Information är en viktig tillgång för vår organisation. För att skydda de värden som informationen representerar krävs ett säkerhetsmedvetande.
Du som är användare får tillgång till Surahammars kommuns nätverk och verksamhetssystem för att underlätta ditt arbete. Alla användare har ansvaret för att resurserna används professionellt, etiskt och enligt lag.
Du får även tillgång till Internet och e-post/konferenssystem som skall användas i rent arbetssyfte. Användandet av e-post/konferenssystem och Internet kan återkallas vid missbruk.

För att leva upp till de säkerhetskrav som ställs på dig måste du känna till:

- Vilket ansvar du har
- Vad du skall göra vid olika incidenter
- Var du skall få stöd och hjälp

It -och telefonisupport

Tel. 670020
helpdesk@vmkfb.se
www.vmkfb.se/surahammar

Behörighet

Surahammars kommuns nätverk och datasystem är utrustade med behörighetskontrollsystem för att säkerställa att endast behöriga användare kommer åt informationen.
För att bli behörig användare krävs din chefs godkännande. DU ansvarar sedan för att följa de regler och riktlinjer som kopplas till behörigheten.

Därefter får du:

- Användaridentitet
- Ett initialt lösenord

Initialt lösenord

Första gången du loggar in på nätverket använder du ett initialt lösenord som du får av helpdesk. När du kommit in i systemet skall du genast byta till ett personligt lösenord, som du själv konstruerar.
Genom detta säkerställs att det bara är du som känner till ditt personliga lösenord.

Personligt lösenord

Lösenordet är strängt personligt och skall hanteras därefter. Du skall därför:

- Inte avslöja ditt lösenord för andra eller låna ut din behörighet
- Skydda lösenordet väl
- Omedelbart byta lösenord om du misstänker att någon känner till det.
- Lösenordet skall bytas minst var 140:e dag om inget annat anges. I vissa system får du en automatisk påminnelse om detta.

Ditt konto är personligt och får endast användas av dig. Det innebär att du inte får lämna (låna) ut det till någon annan. Du får inte heller nyttja någon annans konto.

Du är ansvarig för den trafik som härrör kontot och skall alltså bevara lösenordet för dig själv (jfr PIN kod till bankkort t ex.). Om ditt lösenord kommer på avvägar skall du utan dröjsmål anmäla detta till helpdesk så att lösenordet kan ändras.

Konstruera lösenord

Lösenord måste vara uppbyggda så att de inte går att gissa sig till. Samtidigt får inte lösenordet vara så komplicerat och svårt att komma ihåg att det måste skrivas upp på en lapp som obehöriga kan komma över.

Lösenordet ska konstrueras så att det inte lätt går att koppla till dig som person och minst innehålla minst 7 tecken och innehålla 1 stor bokstav, 1 liten bokstav och en siffra. Enkla mönster som t ex ”ABC 123” eller ”AAAAA2” skall undvikas, liksom alla andra lättforcerade lösenord, såsom eget eller familjemedlems namn eller lösenord av typen QWERTY, dvs., enkla tangentbordskombinationer.

För att skapa bra lösenord kan du t ex:

- Ta första (andra/tredje/sista) bokstaven i en för dig bekant textsträng, melodi eller en boktitel t ex ”SMBFML” från ordspråket ”Som Man Bäddar Får man Ligga”

- Du kan också välja en meningslös uttalbar sekvens, t ex BAMROK

- ”Ovanliga ord” ur ordlistan blandat med en siffra kan också gå bra

Tidigare använda lösenord
Du kan inte återanvända tidigare använda lösenord inom en viss tid. När du byter lösenordet till nätverket kontrollerar systemet att du inte använder något av de 4 senast använda lösenorden.

Bortglömda lösenord
Om du försöker logga in till nätverket med felaktigt lösenord kommer du inte in i systemet. Om detta inträffar vänder du dig till helpdesk. Du kommer då att få ett nytt initialt lösenord.

Kommunens nätverk
I Surahammars kommun anses det som oetiskt när någon:

- försöker få tillgång till nätverksresurser utan att ha rätt till det
- försöker dölja sin användaridentitet
- försöker störa eller avbryta den avsedda användningen av nätverket
- uppenbart slösar med tillgängliga resurser (personal, maskinvara, bandbredd eller programvara)
- försöker skada eller förstöra information
- göra intrång i andras privatliv
- försöker förolämpa eller förnedra andra

Egen utrustning får ej anslutas i kommunens nätverk eller mot Internet.

Loggning
När du är inloggad och arbetar i systemen lämnar du spår efter dig. Systemens loggningsfunktion används för att spåra obehöriga intrång. Detta görs för att skydda informationen och för att undvika att oskyldiga misstänks om oegentligheter inträffar.

Särskilda regler för verksamhetssystem
Om du arbetar specifika verksamhetssystem är det din skyldighet att ta reda på
vad som gäller.
Hanteringen av känsliga uppgifter i dessa system kan kräva striktare regler för t ex Inloggning.

Säkerhetskopiering
I princip all information skall lagras på de centrala servrarna som du har tillgång till.
Detta för att dessa säkerhetskopieras varje dygn. Om du av någon anledning väljer att lagra information på din egen hårddisk måste du själv svara för säkerhetskopiering.

Verksamhetskritisk information skall alltid lagras på lagringsutrymmen på servrar avsedda för detta.
För att förstöra gemensam information krävs ett beslut (se avsnitt om Gallring)

Varje användare har dessutom tillgång på en filserver till en egen hemkatalog. IT-gruppen svarar för att automatisk säkerhetskopiering görs på alla gemensamma servrar.
Vänd dig gärna till IT-gruppen om du är osäker på hur eller var du skall lagra din information.

Att lagra lokalt
För den information som du lagrar lokalt (på din egen dator) ansvarar du själv, vilket innebär att:

- du själv måste ta säkerhetskopior
- du skall tänka på att andra kan ha otillbörligt intresse av att komma över informationen

Internet

Kommunens nätverk är anslutet till Internet via en s k brandvägg som registrerar in- och utgående trafik. All trafik genom brandväggen loggas. Loggen kan sedan granskas om man misstänker oegentligheter.

Modemuppkopplingar mot Internet från datorer som ansluts till kommunens nätverk är inte tillåtet.

Användande av Internet

Vid användande av Internet gäller följande:

- Spelprogram/filmer för privat bruk får inte laddas in i kommunens nätverk
- Gratisprogram får inte laddas in i kommunens nätverk utan att de testats och godkänts av IT-gruppen
- Allmänt gäller vid nedladdning av filer från Internet att du har gott omdöme endast hämtar sådant som är relevant för arbetet och kommer från välrenommerade webbplatser.
- Det är inte tillåtet att via Internet titta/lyssna på material av pornografisk, rasistisk eller nazistisk karaktär. Förbudet gäller även material som är diskriminerande eller har anknytning till kriminell verksamhet eller satanism. Undantagsfall kan vara om det är relevant för arbetet.
- När du surfar på Internet representerar du Surahammars kommun. Agera enligt kommunens värderingar så att det du förmedlar på Internet inte skadar oss. Kom ihåg att du alltid lämnar spår efter dig i form av kommunens ip-adress.

Missbruk av Internet

Exempel på missbruk av Internet ser du nedan. Missbruk kan i vissa fall leda till rättslig påföljd

- Spam, massutskick via e-post
- Köpa saker för privat bruk på Internet
- Dataintrång
- Kedjebrev, pyramidspel
- Att skicka mailbomber, dvs att skicka många mail samtidigt i syfte att skada
- Att skicka e-post som är kränkande eller hotfull
- Att trakassera andra via e-post eller i andras gästböcker
- Att spela spel över Internet
- Att titta på film som inte är relaterad till arbetet

Office 365

Som anställd i Surahammars kommun har du tillgång till detta i MS Office 365

Microsoft Onedrive Pro – Används för lagring av dokument

Office Web Apps – Word, PowerPoint, Excel och OneNote i webbläsaren.

Beroende på vilken typ av licens du har får du tillgång till:

Office installation – Word, PowerPoint, Excel, Outlook och OneNote som du kan installera på din dator.

Office 365 via webinloggning

Skype för företag (Lync) – Kommunikationsverktyg, chatt, videosamtal mm.

I Office 365 har du möjlighet att spara och dela filer online. Office 365 är en så kallad molntjänst, vilket innebär att filer och information sparas på annan plats, dvs. utanför VMKF:s interna servermiljö.

Konton i Office 365 skapas av VMKF:s IT-avdelning, utan att du som användare behöver göra någonting. Inga personliga avtal upprättas mellan användare och leverantören Microsoft. Grundinformation om den anställde hämtas från våra personaladministrativa system.

Inloggning

Du kommer åt Office 365 genom att logga in via länken portal.office.com.
Du loggar in med dina vanliga inloggningsuppgifter, dvs. din e-postadress och lösenord till nätverk du fått av arbetsgivaren. När du ändrar ditt lösenord på datorn måste du även logga in på nytt till portalen

Viktigt att tänka på!

Inga känsliga uppgifter får skrivas eller sparas i Office 365. Material innehållande känsliga uppgifter, såsom till exempel personuppgifter, journaler inom vården och liknande ska hanteras i de system som är avsedda för detta (t.ex. Procapita eller Pulsen Combine).

Alla arbeten och allt material som ska sparas över tid ska sparas på våra interna servrar (G:\, F:\ eller H:\)

Hantering av personuppgifter i förhållande till MS Office 365

Endast personuppgifter om användaridentitet och liknande indirekta personuppgifter, t.ex. namn, förvaltningstillhörighet och liknande kan komma att hanteras i Office 365.

Dessa personuppgifter behandlas av arbetsgivaren för fullgörande av sina arbetsuppgifter, bland annat för genomförande av kommunikation och lagring arbetsmaterial. Innehållet är av okänslig karaktär. Enligt 10 § punkten d PuL, får detta ske utan individens samtycke.

Privatanvändning

Kommunens e-postsystem ska användas i tjänsten. Dock tillåts privat användning i mycket begränsad omfattning.

Allmän handling

För att allmänheten utnyttja sin rätt att ta del av allmänna handlingar är det viktigt att man få veta vilka handlingar som finns hos myndigheten.
Allmänna handlingar är i princip alla handlingar som finns hos kommunen och anses vara inkommen till kommunen eller upprättad hos kommunen.

Allmänna handlingar är antingen offentliga eller hemliga. Huvudregeln är att allmänna handlingar är offentliga men inom vissa verksamheter t ex socialtjänst är de flesta handlingar hemliga.

För att upprätthålla offentlighetsprincipen måste handlingar registreras, diarieföras.

Kraven på vad som ska diarieföras skiljer sig inte åt beroende på om handlingen finns på papper eller i dataform. Detta innebär att t ex även e-post räknas som en inkommen handling så snart den kommit till kommunen.
Av stor vikt att komma ihåg att med kommunen avses i detta sammanhang alla verksamheter, om en handling kommer till kommunkontoret en skola, ett äldreboende eller annan enhet har ingen som helst betydelse för kravet på diarieföring.

Vad ska då diarieföras? I princip ska allt diarieföras som inte är av ringa betydelse i lagstiftningens mening. Med ringa betydelse avses t ex reklam, kursinbjudningar etc. Vidare behöver man inte diarieföra / registrera under förutsättning att det går att göra material sökbart på något annat sätt. Den sistnämnda möjligheten gäller dock inte för hemliga handlingar, de måste alltid diarieföras.

Gallring

Gallring är detsamma som utrensning av information som bedöms vara mindre betydelsefull i ett långtidsperspektiv.
Det innebär att gallring alltid skall föregås av en informationsklassning där informationen värderas utifrån krav från lagstiftning och verksamhet.
Allmänna handlingar får inte förstöras utan ett gallringsbeslut.

I Surahammars kommun får du radera

- E-post av mindre betydelse
- Cookie-filer och temporära Internet-filer efter inaktualitet

Datavirus

Datavirus kan sägas vara 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 eller serverns hårddisk.

Virus är ofta ytterst smittsamma och ”smittkällan” kan vara svår att identifiera.
Gratisprogram, spelprogram, och filer som laddas ned från Internet eller filer som följer med e-postmeddelanden är vanliga smittbärare.

I Surahammars kommun har vi virusprogram som automatiskt uppdateras vid alla arbetsplatser. Om du har frågor angående virusskyddet på din dator, arbetsplats
eller misstänker att din dator har smittats av virus skall du kontakta IT-gruppen.

Tecken på datavirus

Datorns virusprogram talar om att du har virus.
Datorn uppför sig på ett onormalt sätt t ex tecken flyttar sig, förändringar på skärmen
Datorn arbetar mycket långsamt

Om du misstänker att du drabbats av virusskall du:

- Avbryta allt arbete
- Stänga av datorn
- Se till att ingen annan använder datorn
- Omedelbart kontakta helpdesk

Incidenter

En incident kan vara i stort sett vad som helst: från besökare på villovägar, olåsta dörrar och misslyckad säkerhetskopiering, till driftavbrott, försök till dataintrång och virusangrepp.

En incident kan vara en medveten handling eller ske helt oavsiktligt. Någon glömmer t ex att låsa en dörr eller säkerhetskopiera en server.

Säkerhetsincidenter och brister som kan utgöra ett hot mot säkerheten måste snarast möjligt rapporteras. Kontakta helpdesk om du t ex:

- Misstänker att någon använt din användaridentitet
- Upptäcker svagheter och brister i IT-system/program
- Misstänker virus, stöld, brand eller sabotage etc.

Om du misstänker att någon obehörig har använt din användaridentitet och varit inne i systemet:

- Notera tidpunkt då du själv var påloggad i systemet
- Notera tidpunkt då du upptäckte förhållandet
- Anmäl omedelbart till helpdesk
- Skriv ner alla iakttagelser och försök se om information i systemet förändrats eller förstörts

Om du får hotfulla, kränkande brev eller e-post skall du inte radera dessa.
De är bevismaterial om du väljer att polisanmäla eller kontakta IT-gruppen för hjälp.

Alla medarbetare i organisationen samt extern personal som utför uppdrag för kommunens räkning skall rapportera inträffade IT-incidenter och upptäckta säkerhetsbrister till helpdesk. IT-ansvarig skall upprätta en incidenthanteringsplan samt sammanställa och analysera de incidenter som inträffar. It-incidenthanteringsplanen skall utgöra en del av kommunens säkerhetspolicy.

Arbetsplatsen

Ordning reda på arbetsplatsen är viktig för säkerheten.

Om du lämnar arbetsplatsen bör du logga av även om det bara är en kortare stund.
Lämnar du arbetsplatsen mer än 15 minuter skall du logga av.
Om du glömmer att logga av är det risk att obehöriga kommer åt informationen.

Kom ihåg att du ansvarar för allt som registreras med din användaridentitet.

Utskrifter på gemensamma skrivare ska hämtas så snart som möjligt. Tänk på att kvarglömda dokument kan komma i orätta händer.

Se till att datorer som innehåller känslig information inte står placerade så att obehöriga kan läsa vad som står på skärmen.

Om din dator behöver service lämnas den alltid till helpdesk.

Mobil datoranvändning och distansarbete

Mobil datoranvändning

Användning av bärbar IT-utrustning innebär särskilda risker, i synnerhet om de används på oskyddade platser som konferenslokaler, flygplats eller hotellrum

Därför bör du:

- Alltid hålla utrustningen under uppsikt om du inte kan låsa in den
- Inte lagra verksamhetskritisk information på utrustningen
- Inte exponera känslig information vid arbete på t ex tåg
- Alltid förvara en säkerhetskopia på din arbetsplats
- Förvara utrustning säkert även i bostaden
- Inte låta anhöriga eller vänner nyttja den bärbara utrustningen

- En dator som anslutits till ett annat nätverk skall alltid ha ett av kommunen installerat eller godkänt virusskydd

Distansarbete från hemmet mot verksamhetssystem eller lokal lagring annan plats får endast ske efter överenskommelse med din chef.

Ordlista

Användaridentitet	Unik identitet för en person som utnyttjar vårt datasystem
Behörighet	Rättighet för användare att använda dataresurser
Behörighetskontroll	Åtgärder för kontroll av användaridentitet
Bifogade filer	Dokument som skickas med koppling till e-post
Brandvägg	Hinder mot oönskat intrång i vårt nätverk
Cookies	Liten datamängd med information om tidigare besök som en webbserver skickar till en webbläsare och sedan kan hämta information ifrån
Dataintrång	Obehörig tillgång till information i datasystem
Datasystem	Innefattar datorer, servrar, program mm
Diskutrymme	Utrymme data tar på en hårddisk
Filserver	En dator där man lagrar data som kan nås av flera användare
Gratisprogram	Program som man kan använda utan att betala licenskostnad
Hemkatalog	Din egen lagringsplats på servern
Hårddisk	Enhet i din dator eller server som lagrar data
Internet	Ett internationellt datornätverk
Klient	Den anställdes dator
Logg	Kontinuerligt insamlad information om det som händer händer i ett datasystem
Loggning	Förande av logg
Mailbomber	När en stor mängd e-postmeddelanden samtidigt skickas till en e-postserver i syfte att skada
Nätverk	Ett antal datorer som på något sätt är sammanbundna och kan kommunicera med varandra
Program	Instruktioner lagrade i datorn och styr dess funktioner
Server	En mer kraftfull dator som används av flera klienter
Shareware	Program som får spridas fritt men som användaren förväntas betala en avgift för vid upprepad användning

Snabela	Tecknet@. Används i e-postadresser
Spam	Skräpmail eller massutskick
Surfa	Besöka webadresser på Internet
System	Komponenter som på något sätt är förbundna med varandra
Systemansvarig	Utses av systemägare och ansvarar för hantering av system
Säkerhetskopia	Kopia av fil eller annan data som sparas om originalet blir förstört
Temporära Internet-filer	Används för att spara webbsidor eller bilder medan du tittar på dem. Detta gör att det går fortare att visa tidigare besökta hemsidor
Verksamhetssystem	System som används för att effektivisera eller på annat sätt förbättra verksamhet.
Vidarekoppling	Automatisk vidaresändning av e-post
Webbläsare	Datorprogram för visning och hämtning av information
Webbsida	Den mängd information på en webplats som man kan se på skärmen samtidigt eller genom att rulla bilden