Diarienummer
KS-2/24

Normerande styrdokument

Riktlinjer för it-användare

Policy

Riktlinje

Rutin/väg-ledning

HALLSTAHAMMARS KOMMUN

Beslutad av: Kommunstyrelsen

Datum och paragraf: 2024-01-22 $4

Giltighetstid: 2024-2025

Revideringar och omarbetningar: En ggr/år

Policy

Riktlinje

Rutin/väg-ledning

Dokumentet gäller för: Samtliga som ges behörighet till Hallstahammars kommuns it-miljö

Dokumentansvarig: IT-strateg, enheten för strategisk utveckling och planering

Innehåll

Policy

Riktlinje

Rutin/väg-ledning

Riktlinjer för it-användare

Riktlinjerna beskriver det ansvar man som medarbetare vid hantering av information och it-utrustning i Hallstahammars kommun och vilka regler som gäller.

Hallstahammars kommun är en organisation med många skilda verksamheter. Kompletterande regler till riktlinjerna kan därför finnas lokalt. Avvikelser från dessa riktlinjer får dock aldrig göras utan särskilt tillstånd. Kontakta ansvarig chef vid osäkerhet om vad som gäller.

E-post

E-post är för många medarbetare det vanligaste och viktigaste sättet att kommunicera internt inom Hallstahammars kommun och till externa parter. E-postens lagringskapacitet är begränsad. Tänk på att regelbundet radera i mapparna ”Inkorgen”, ”Skickat”, och ”Borttaget”. Innan du raderar e-post måste du förvissa dig om att allmänna handlingar är hanterade.

E-postsystemet ska inte användas som ett arkivsystem utan är endast ett transportsystem. All information som ska bevaras, såsom meddelanden, bifogade filer med mera, sparar du på samma sätt som du lagrar annan information. Som filer på dina lagringsplatser eller i aktuellt förvaltningssystem.

Dataskyddsförordningen styr hur vi får använda och behandla personuppgifter i samhället. Förändringen påverkar även vår e-posthantering och kräver att vi förändrar vårt arbetssätt och våra rutiner kring hantering av personuppgifter i e-post.

Grundregel: Hantering av personuppgifter ska främst ske i förvaltningssystem, inte i e-post. Hantering av personuppgifter i e-post räknas också som behandling av personuppgifter och samma krav gäller som för alla andra behandlingar. Läs mer om vad som gäller på www.imy.se.

E-post, ansvar

- Den enskilde medarbetaren som är kontoinnehavare för ett personligt e-postkonto är alltid ansvarig för den e-post som skickas från kontot.
- Medarbetare är ansvarig för att löpande öppna och läsa inkommande e-post. Vid frånvaro, t.ex. semester, sjukfrånvaro eller föräldraledighet, ska autosvar användas med hänvisning till kollega eller chef. Om automatisk vidarebefordring av e-post används ska den gå till en delad e-postlåda som kan läsas av flera.
- E-postkonton som delas av flera, t.ex. myndighetsbrevlådor (för nämnder) och funktionsbrevlådor (t.ex. för enheter) ska ha utpekade ansvariga.
- Under vissa förutsättningar är det tillåtet för medarbetare att synkronisera och visa e-brevlåda och kalender i privat telefon eller surfplatta.
  Dessa förutsättningar är:
  - Smartphonen/surfplattan får inte vara ”jailbreakad/rootad”, det vill säga illegalt upplåst enhet.

- Medarbetaren får inte själv lagra någon arbetsrelaterat från mejl eller kalender på den privata smartphonen/surfplattan.

E-post, allmänna handlingar

- E-post som skickas till personliga brevlådor är allmän handling om innehållet är arbetsrelaterat. Vid arbetsrelaterad e-post ska alltid regler för registrering och hantering av allmänna handlingar följas. Huvudregeln är att e-post som är allmän handling omgående ska vidarebefordras till registrator.
- E-post som är allmän handling får gallras, dvs. raderas, först när e-posten registrerats och eller diarieförts. Vissa e-postmeddelanden som är allmänna handlingar är av uppenbar ringa eller tillfällig betydelse och är undantagna från kravet på registrering. Dessa får gallras i enlighet med Hallstahammars kommun gallringsregler.

E-post, privat

- Håll isär arbetsrelaterad, i annan ställning och privat kommunikation när du kommunicerar via e-post. Använd inte ditt e-postkonto i Hallstahammars kommun för privata ändamål. Privat e-post ska du hantera i en privat e-brevlåda där du inte hanterar arbetsrelaterade meddelanden.
- Viktig information ska lagras på kommunens nätverk där säkerhetskopiering sker kontinuerligt. Det är inte tillåtet att lagra viktig information enbart på en mobil enhet.
- Enheten får enbart anslutas till trådlösa nätverk som är kända och lösenordskyddade.
- Privat utrustning kan anslutas till Hallstahammars kommuns gästnätverk.

Säker e-post, personuppgifter och sekretess

E-post är en elektronisk kommunikationsmetod som inte alltid är säker. När du skickar ett e-post går det vanligtvis igenom flera servrar innan den når mottagaren. Under denna process kan någon med tillräckligt teknisk kunskap avlyssna e-postmeddelandet och få tillgång till de uppgifter som finns i meddelandet.

Detta är anledningen till att det är viktigt att skicka känsliga personuppgifter och sekretess via säker krypterad e-post. Kryptering är en metod som gör det möjligt att koda informationen så att den endast kan avkodas av den person som har rätt nyckel för att öppna den. Denna lösning brukar benämnas som säker e-post.

Skicka aldrig känsliga personuppgifter eller sekretess via vanlig e-post. Läs mer om hur du använder säker e-post på intranätet.

Policy

Riktlinje

Rutin/väg-ledning

Skadlig kod

Skadlig kod är ett samlingsbegrepp för oönskade datorprogram som virus, trojaner, spionprogram och maskar. Dessa kan installeras på en dator eller ett nätverk utan administratörens samtycke. Skadligkod har utvecklats i syfte att störa it-system, för att samla in information eller för att utnyttja datorkraft eller minneskapacitet i it-utrustning.

Skadlig kod är ett växande problem då koden blir mer och mer sofistikerad och ”intelligent”. I och med det blir den svårare att upptäcka och kan hinna göra större skada innan den oskadliggörs. Man behöver idag inte vara en teknisk kunnig hacker för att skapa skadlig kod, utan det mesta kan köpas och beställas på olika marknadsplatser på internet.

Exempel på förekommande skadlig kod:

- Vissa trojaner, s k keyloggers, kan avlyssna lösenord och skicka dessa vidare.
- Det finns trojaner som skapar bakdörrar i datorer så att andra personer får tillgång till dessa utan ägarens vetskap. Syftet kan vara att lagra olaglig information.
- Ett ökande problem är så kallad ransomware där filer eller diskar på dator (eller smart mobil eller surfplatta) krypteras och man sedan krävs på en lösensumma för att enheten ska låsas upp.

Spridning av skadlig kod

Skadlig kod kan spridas till ens dator eller mobila enhet om man öppnar bilagor i e-post, importerar filer eller surfar på internet och klickar på fel länkar. Detta gäller även sociala medier.

Avsändare till e-post kan vara falska och webbsidor är inte alltid vad de utger sig för att vara. Identiteter kan kapas, till exempel på Facebook, och e-postadresser kan förfalskas i syfte att lura mottagaren att klicka på länkar. Vid så kallad Phishing luras mottagaren att klicka på en länk som leder till en sida där man ombeds fylla i koder, lösenord eller bankkonton. Var observant på detta och fylla aldrig i sådana uppgifter! Seriösa myndigheter, företag och andra organisationer ber aldrig om uppgifter på detta sätt.

It-utrustning som drabbats av skadlig kod, även ett smittat usb-minne, kan om det kopplas upp i Hallstahammars kommuns nätverk, sprida sig vidare i nätverket och orsaka stor skada.

Hallstahammars kommuns datorer är utrustade med skydd mot skadlig kod. Detta innebär inte fullständig säkerhet då utvecklingen inom detta område är oerhört snabb. Alla medarbetare kan också bidra till ett bra skydd mot skadlig kod genom att följa dessa regler:

- Stäng aldrig av eller på annat sätt inaktivera installerat skydd mot skadlig kod.
- Anslut endast it-utrustning ägd av arbetsgivaren till Hallstahammars kommuns nätverk.

- Var misstänksam och undvik att klicka på konstiga länkar. Fyll heller inte i irrelevanta eller ologiska uppgifter som efterfrågas. Ha ett kritiskt granskande öga och var inte alltför godtrogen.
- Öppna bifogade filer endast om de kommer från en känd avsändare och om bilaga är förväntad.
- Var observant på om it-utrustning beter sig långsamt eller konstigt. Vid misstanke om skadlig kod kontakta servicedesk.

Internet

Användning av internet är till stor nytta och glädje, privat såväl som på arbetet. Förutom de riktlinjer som är kopplade till skadlig kod finns här särskilda regler för användning av internet.

- Internet är främst ett arbetsverktyg och ska inte störa ordinarie arbetsuppgifter eller innebära merkostnader för arbetsgivaren.
- De regler som gäller i samhället i övrigt gäller självklart även inom Hallstahammars kommun. Tryckfrihetsförordningen, brottsbalken, lagen om upphovsrätt samt dataskyddsförordningen är exempel på lagar som ibland måste beaktas när man använder internet.
- För material på internet som ska användas i tjänsten, får nedladdning och installation av upphovsrättsligt material (datorprogram, film, musik, bilder med mera.) inte ske utan stöd i lag, avtal eller med skriftligt tillstånd från rättighetsinnehavaren.
- I begränsad omfattning får internet användas för privata syften. Utrymmeskrävande filtyper såsom filmer, program och spel får dock inte för privat bruk laddas ned, strömmas, lagras eller spridas i eller via kommunnätverket.
- Internet är ett öppet nätverk och endast öppen information får publiceras eller delas, alltså inte intern eller konfidentiell information.
- Det är inte tillåtet att besöka webbplatser med till exempel brottslig verksamhet, rasism, diskriminering, extrempolitiskt eller pornografiskt innehåll. All internettrafik loggas och stickprov kan komma att utföras.

Lagring

En av de grundläggande principerna i dataskyddslagstiftningen är principen om lagringsminimering, det vill säga att samla in så få personuppgifter som möjligt. Du får bara samla in de uppgifter som behövs för att kunna utföra arbetet.

Det är viktigt att information lagras på ett säkert sätt och säkerhetskopieras så att den kan återskapas i händelse av diskkrasch, oavsiktlig radering med mera.

Lagring, regler

- Information ska lagras på nätverket så att den säkerhetskopieras. Lagringen kan ske antingen på en personlig nätverksplats eller på gemensamma filareor, beroende på vad som ska lagras.
- Om information behöver lagras på lokal hårddisk, se till att regelbundet kopiera över informationen till nätverket.
- Information som omfattas av sekretess får endast lagras i därför avsedda och godkända system och lagringsytor. Systemen och lagringsytorna ska ha begränsad åtkomst både vad gäller användare och administratörer.
- Endast godkända molntjänster är tillåtna att användas. Kontrollera vilka molntjänster som är tillåtna inom din verksamhet. Exempel på molntjänster och molnlagring som inte får användas är Dropbox.
- Information som omfattas av sekretess får inte lagras i molntjänster.

Lagring, personuppgifter

Vid behandling och lagring av personuppgifter ska följande dokumenteras:

- Ändamål för behandlingen.
- Vilket lagligt stöd som används.
- Vem eller vilka som har tillgång till informationen och i vilket syfte.

Spårbarhet och loggning

Loggning sker i Hallstahammars kommuns datorer och nätverk. Loggarna används för felsökning och för utredning av incidenter eller för att förhindra brott. Loggarna lagras under en viss tid, och är åtkomliga endast för en begränsad grupp administratörer.

Spårbarhet innebär att man genom loggning kan identifiera vem som har gjort vad och när samt följa förloppet för olika händelser på datorn.

All internettrafik och e-post loggas centralt. Hallstahammars kommun, som arbetsgivare har rätt att, utan att meddela användaren, gå igenom dessa loggar för att kontrollera efterlevnad av lagstiftning och riktlinjer. Vid misstanke om brott kan loggfilerna komma att lämnas ut till rättskipande myndighet utan att du som kontoinnehavare meddelas.

Sociala medier

Gå igenom *Riktlinjer för användning av sociala medier i Hallstahammars kommun* för att ta del av vad som gäller.

Konton och behörigheter

Informationssystem inom Hallstahammars kommun är utrustade med behörighetskontrollsystem för att säkerställa att endast behöriga användare kommer åt information. De behörigheter du blir tilldelad beror på dina arbetsuppgifter och bestäms av din chef. I Hallstahammars kommun skapas ett grundkonto (AD-konto) med automatik som ger dig tillgång till e-post och en lagringsyta. Din närmaste chef får dina

uppgifter skickade till sig. Tillgång till övriga konton och behörigheter till förvaltningssystem som medarbetare behöver beställs av närmaste chef. Beställningar görs hos respektive systemadministratör.

Lösenord

Som användare av it-resurser i Hallstahammars kommun ansvarar du själv för att dina lösenord håller den kvalitet som beskrivs i detta dokument. Du håller dina lösenord hemliga, och som konsekvens av detta aldrig uppger dina lösenord för någon, även om de efterfrågar dem. Ingen har rätt att begära dina lösenord, och du har inte rätt att uppge dem.

Lösenord, regler

- Dina lösenord ska vara starka. Starka lösenord kan skapas antingen genom att kombinera enskilda tecken till ett relativt kort men komplext lösenord.
- Ett komplext lösenord består av minst åtta slumpmässigt valda tecken och ska innehålla versaler, gemener, siffror och specialtecken. Tecknen ska inte väljas med någon systematik. Att exempelvis ta första bokstaven ur flera ord, eller ändra vissa bokstäver till siffror i ett ord är inte lämpligt, eftersom detta leder till förutsägbara mönster. Använd inte svenska tecken (å,ä och ö) i lösenordet.
- Använd olika lösenord till olika system. Använd enbart dina arbetsrelaterade lösenord för inloggningar till system och tjänster som du använder i ditt arbete. När du loggar in i system eller på webbsidor privat ska du använda andra lösenord.
- Det är tillåtet att skriva upp lösenord. Uppskrivna lösenord ska förvaras på ett säkert ställe, utan information om vad de används till.
- Om ditt lösenord blir känt av andra måste du byta det.

Hallstahammars kommun har en lösenordsportal där du som användare kan logga in om du vill byta eller glömt ditt lösenord. Lösenordsportalen hittar du på intranätet.

Programvaror och appar

Egna program får inte installeras i arbetsgivarens datorer eller på andra enheter. Det är inte tillåtet att kopiera eller använda program som arbetsgivaren tillhandahåller utanför ordinarie verksamhet. Vid behov av ytterligare programvaror eller hårdvara anmäls detta till närmaste chef.

Egna enheter

Egna enheter får tas med till arbetet. Dessa kan anslutas till Hallstahammars kommuns öppna nätverk. Inget arbetsmaterial får lagras direkt på den egna enheten.

Policy

Riktlinje

Rutin/väg-ledning

Distansarbete

För att komma åt gemensamma lagringsytor eller interna system används en VPN uppkoppling till Hallstahammars kommuns It-miljö. Varje verksamhetschef avgör om det

är tillåtet med distansarbete på arbetsplatsen och dokumenterar om det finns några särskilda reservationer eller regler för detta. Alla bärbara datorer (laptops) är försedda med en vpn-klient, dock krävs det en specifik behörighet för att anslutningen ska fungera. Behörigheten beställs av närmaste chef.

Säkerhet på arbetsplatsen

Ordning och reda där du befinner dig när du arbetar (arbetsplatsen) är viktig för säkerheten.

Förhållningsregler

- Om du lämnar arbetsplatsen ska du låsa datorn även om det bara är en kortare stund (detta kan enkelt göras med Windows tangenten + L)
- Om du glömmer att låsa datorn är det risk att obehöriga kommer åt informationen och är då att betrakta som en incident som ska rapporteras.
- 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. Utskrift av känsliga eller sekretessbelagda uppgifter får bara ske med så kallad säker utskrift (inget skrivs ut innan du kvitterat utskriften vid skrivaren).
- Se till att datorer som innehåller känslig information inte står placerade så att obehöriga kan läsa vad som står på skärmen.

Riskminimera åtkomst till känsliga uppgifter genom att

- Ta reda på om det finns några filer lokalt på datorn som innehåller känsliga uppgifter (personuppgifter, sekretess).
    - Alla filer som ligger på C: ligger lokalt på datorn. Tänk på att det som ligger på datorns skrivbord, i papperskorgen och i hämtade filer (det du har laddat hem från nätet eller system) ligger lagrade på datorn
    - Om det finns känsliga uppgifter lokalt på datorn, identifiera dessa, gör en riskbedömning och vidta eventuella åtgärder.
- Om du upptäcker att du har behörighet till filer eller system som du inte borde ha behörighet till, meddela din chef.

Om din digitala enhet försvinner

Våra digitala enheter (exempelvis datorer, telefoner och surfplattor) innehåller ofta personuppgifter eller är kopplade till system som innehåller personuppgifter eller annan känslig information. Därför är det viktigt att snabbt spärra åtkomsten till kommunens nätverk och därmed kopplingen till flera system som enheten kan ha åtkomst till när en enhet försvinner.

- Anmäl att den digitala enheten är försvunnen till itsupport@hallstahammar.se. Meddela datornamn/serienummer eller vem som senast var inloggad på enheten och när enheten försvann. Enheten spärras då och kan inte längre användas för att logga in i kommunens nätverk och de system som är kopplade till detta.

- Gör en anmälan om personuppgiftsincident via e-tjänsten på intranätet och följ rutinen för personuppgiftsincident.
- Ta reda på vilka känsliga uppgifter som finns på enheten (se avsnitt ovan Riskminimera åtkomst till känsliga uppgifter genom att), gör en riskbedömning för dessa och vidta lämpliga åtgärder.
- Gör en polisanmälan om enheten är stulen.

Servicedesk

Behöver du hjälp med it-relaterade frågor kan du kontakta servicedesk på telefon 0220 - 246 00 eller e-posta support@iver.se