Svar på medborgarförslag om porrfri barndom

35

2021KS295

Kommunstyrelsen

Datum
2021-12-20

Diarienummer
2021KS295 009

Svar på medborgarförslag om porrfri barndom

Förslag till beslut

Kommunstyrelsen anser medborgarförslaget besvarat.

Sammanfattning av ärendet

Kommunfullmäktige beslutade den 20 maj 2021 § 106 att till kommunstyrelsen remittera ett medborgarförslag om en porrfri barndom. Kommunfullmäktige uppdrog till kommunstyrelsen att besluta i ärendet.

Medborgarförslaget handlar om förslag på hur kommunen kan jobba med porrprevention, framför allt i de verksamheterna som arbetar med barn. Förslagsställaren lyfter fram två punkter som viktiga i det aktiva arbetet med porrprevention:

- Installera porrfilter/teknisk lösning på kommunens digitala enheter och wifi-nätverk i verksamheter där kommunen och huvudman
- Införa porrfri policy om att det inte är acceptabelt att spela upp nätpornografi varken via kommunens nätverk, kommunens digitala enheter eller privat teknisk utrustning som t.ex privat smartphone på de verksamheter som kommunen är huvudman och barn vistas.

Beträffande den första punkten i förslaget har förvaltningen i november 2021 slutfört installation av webbfilter mot porr som omfattar samtliga verksamheter. Användare som ansluter via kommunens nätverk skyddas genom filtret. Alla datorer och telefoner som hanteras av IT-funktionen omfattas dessutom av skyddet när de används utanför kommunens nätverk.

I dagsläget omfattas inte inloggning via gästportal på kulturhusen av webbfiltret. Förvaltningen arbetar för att åtgärda detta tillsammans med ansvarig leverantör av tjänsten under 2022.

Medborgarförslaget innehåller även förslag på porrfri policy. I *Rutin för informationssäkerhet medarbetare* anges vad som gäller för Härryda kommuns anställda:

”När du surfar på internet representerar du Härryda kommun och lämnar spår efter dig i form av Härryda kommuns IP-adress.

Det är inte tillåtet att via internet ta del av eller publicera material av pornografisk-, rasistisk-, eller förtroendeskadlig karaktär. Förbudet gäller också material som är diskriminerande eller har anknytning till kriminell verksamhet eller på annat sätt oförenligt med svensk lagstiftning.”

Porrfilter och policy är en del i arbetet för en trygg skolmiljö men behöver kompletteras med kunskap och diskussion. Inom ramen för skolans värdegrundsarbete är det viktigt att lyfta frågor och ge eleverna möjlighet diskutera ämnen som ibland kan vara kontroversiella eller känsliga. Det är en viktig del av skolans uppdrag att personal kan problematisera frågor som exempelvis pornografi.

Förvaltningen bedömer att det webbfilter som installerats i kommunen samt befintlig rutin för informationssäkerhet motsvarar det som efterfrågas i medborgarförslaget.

Beslutsunderlag

- Tjänsteskrivelse 20 december 2021
- Medborgarförslag om porrfri barndom
- Rutin för informationssäkerhet

Päivi Malmsten
Sektorschef

Elin Rosén
Administrativ chef

Lämna ett medborgarförslag

1. Inlämnat av

Inlämnat av
Personnummer

För- och efternamn
EMMA GUSTAFSSON

Adress

Postnummer och ort

Telefon

E-postadress

Mobiltelefon
-

Notifieringar
E-post

2. Ditt förslag

Rubrik på ditt förslag
Porrfri barndom

Beskriv förslaget
Jag har ett förslag om att kommunen tar sitt ansvar och jobbar med porrprevention, framförallt i verksamheter där vi har barn. I bilaga ser ni förslag till åtgärder som andra kommuner redan har implementerat.

Bifogat material
Här kan du bifoga filer som komplement till ditt förslag. Det kan till exempel vara bilder, ritningar eller dylikt.

Hej-kommun-medborgarförslag.pdf (73 KB)
Samtliga filer ovan finns bifogade i detta dokument, se bifogade filer.

Hej,

Har kommunen infört aktiv porrprevention för barn, enligt de tre punkterna nedan, på platser där barn vistas som kommunen är huvudman för?

På internet har barn enkel tillgång till miljontals gratis porrfilmer som ofta innehåller grov sexism, rasism och våld bl.a. så kallat “strypsex”. Porrindustrins aggressiva marknadsföring når även barn som inte själva söker aktivt efter nätpornografi bl.a. genom pop-up-annonser, enkla sökord t.ex. “xxx” och länkade filmer. Det är även vanligt att barn exponeras genom att ett annat barn visar, det sker ofta i skolan, redan i lågstadiet.

Läkare, psykologer, gynekologer och kriminologer m.fl. vittnar från sitt dagliga arbete med barn om hur nätpornografin genererar en eskalerande fysisk och psykisk hälsokris bland barn. Det är vanligt att barn blir traumatiserade av det grova innehållet i nätpornografin samt att de kopierar det de lär sig i nätpornografin och även utsätter andra barn, ofta utan att förstå att det är fel. Polisen, NOAs, egen kartläggning* visar att skolan är den plats där flest flickor utsätts för sexuella trakasserier utanför hemmet. Barnens MeToo-upprop #kidstoo, #räckupphanden och #tystiklassen innehåller åtskilliga exempel på en utbredd sexuell utsatthet bland barn i skolor. Många tjejer berättar hur killar exponerar dem för nätpornografi mot deras vilja när lärare inte ser, att de trakasseras med referenser från porrfilmer och att de utsätts fysiskt för porrinspirerade övergrepp i skolan. Kommunstyrelsens ordförande i Falkenberg, Per Svensson, meddelar att ett tiotal incidenter har rapporterats per år där killar tvångsvisar nätpornografi för tjejer i skolan och att mörkertalet är stort, något som även rapporteras runt om i landet.

Som kommuninvånare förväntar jag mig att förskola, skola, fritids, bibliotek och andra platser i kommunens regi där barn vistas ska vara vara en porrfri zon. För att porrfria zoner ska bli realitet är det nödvändigt att kommunen inför aktiv porrprevention genom följande punkter:

- **Installera porrfilter/teknisk lösning** på kommunens digitala enheter och wi-fi-nätverk i verksamheter där kommunen är huvudman.
- **Inför porrfri policy** om att det inte är acceptabelt att spela upp nätpornografi varken via kommunens nätverk, kommunens digitala enheter eller privat teknisk utrustning som t.ex. privat smartphone på de verksamheter som kommunen är huvudman för där barn vistas.

Nedan följer:
1. **Argument för porrfria zoner i kommunens allmänna miljöer**
2. **Källor och referat om att det är olagligt att exponera barn för pornografi**
3. **Myter och fakta om teknisk lösning som begränsar kontaktytan, s.k. “porrfilter”**

Jag hoppas på ett gott samarbete och att vi tillsammans kan göra de allmänna platser som kommunen ansvarar för till porrfria zoner för barn. Jag ser fram emot ert svar!

Vänligen,
Kommuninvånare

1. Argument för porrfria zoner i kommunens allmänna miljöer

- Porrfria zoner har ett starkt **normbildande signalvärde**, likt samtyckeslagen, sexköpslagen samt åldersgräns på alkohol och tobak.
- Porrfria zoner **begränsar risken att exponeras** för nätpornografi, framför allt ofrivillig exponering, samt rustar och **stärker elevernas kritiska tänkande** gällande nätpornografi.
- Kommunens verksamhet ska stå för **antivåld, antirasism, jämställdhet och allas lika värde - alltså motsatsen till den vanliga nätpornografin** på samtliga punkter.
- **Det är även olagligt att exponera barn för våld**, mer om det nedan.

2. Källor och referat om att det är olagligt att exponera barn för nätpornografi

- Barnkonventionen blev lag i Sverige 1 januari 2020. Barnets rättigheter i enlighet med **barnkonventionen kräver att vuxna ger barn det skydd från våld som barn har rätt till**. ”Konventionsstaterna skall uppmuntra utvecklingen av lämpliga riktlinjer för att **skydda barnet mot information och material som är till skada för barnets välfärd**, med beaktande av bestämmelserna i artiklarna 13 och 18.” (artikel 17e, unicef.se/barnkonventionen)

  Porrfilter/teknisk lösning är en viktig åtgärd för att förebygga att barns välfärd skadas av information och material som är skadliga för barn, till exempel den vanliga nätpornografin.

- **Porrbilder får inte sättas upp på allmänna platser som till exempel på anslagstavlor. Den som gör det kan dömas till böter eller fängelse.** (Om brott mot allmän ordning, kapitel 16 paragraf 11)

  Digitala bilder och filmer med pornografi på skärmar genererar samma negativa effekter på barn som printade pornografiska bilder.

- **Porrfilmer får inte visas på TV vid tidpunkter då barn brukar titta.** (Radio och Tv-lag (2010:696), kapitel 5 paragraf 2)

  Nätporren finns alltid tillgänglig för barn på internet, dygnet runt, alltså även på tidpunkter då barn brukar titta.

- **Porr får inte innehålla bilder av barn. Den som gör, tittar på, sprider, säljer, ger bort eller gör det möjligt för någon att få tag på barnpornografiska bilder gör något olagligt. Som barn räknas enligt lagen den som är under 18 år.** (Brottsbalken, kapitel 6 sexualbrott paragraf 10)

  Många porrsajter saknar åldersverifiering på de som medverkar i porrfilmerna. Ett flertal barn har identifierats i filmer bl.a. på Pornhub, en av världens mest populära porrsajter. Det förekommer alltså dokumenterade sexuella övergrepp på barn, s.k. “barnporr, även bland s.k. “vuxenporr” på de vanliga porrsajterna.

- **Man får inte sprida porr som visar sexuellt våld eller tvång där någon till exempel riskerar att skadas.** (Brott mot allmän ordning, kapitel 16 paragraf 10 c)

  Forskning visar att 89.8% av alla scener i nätpornografin innehöll fysisk aggression** som bland annat slag, stryptag, “ass-to-mouth” och “gagging”. När journalist och författare Katarina

Wennstam gjorde research bland den vanliga nätporren på de stora porrsajterna fann hon mycket grovt våld, hon skriver bl.a. “Jag har inte alltid varit säker på att hon kommer att överleva tills filmen är slut.”***

3. Myter och fakta om porrfilter/teknisk lösning

Myt: Porrfitler/teknisk lösning tar alltid bort HBTQI-information och sexualupplysningsidor.
Fakta: Det är **enkelt att kontrollera** att ett porrfilter/teknisk lösning inte tar bort sidor med sexualupplysning och HBTQI-information t.ex. umo.se, rfsu.se, rfsl.se och snaf.se. **Det går att korrigera** om en viss webbsida skulle tas bort av misstag.

Myt: Porrfilter/teknisk lösning är kontraproduktivt på grund av att samtalen skulle utebli.
Fakta: Forskning från Uppsala universitet**** visar att nästan inga av barnen i studien hade pratat med en vuxen om pornografi någon gång. Alltså, **samtalen uteblir oftast oavsett om det finns porrfilter/teknisk lösning eller ej - om inte vuxna initierar samtalen**. **Därför är det viktigt att all porrprevention innhåller en helhetslösning som både begränsar tillgången och att barnen får ta del av åldersanpassade regelbunden porrkritisk undervisning och porrkritiska samtal.**

Myt: Porrfilter/teknisk lösning fungerar inte
Fakta: **Porrfilter har en betydande effekt, framför allt risken för ofrivillig exponering** särskilt bland de yngre barnen**. Exempelvis stoppades 10.200 sökningar på pornografiska webbsidor i Karlstads kommunkoncerns nätverk under april 2020.** Vad är definitionen på att “fungera”? Om definitionen av “fungera” är = “100% effekt” är det mycket i kommunens verksamhet som inte “fungerar” men som ändå används på grund av att det har en betydande effekt. Det finns inget porrfilter/teknisk lösning som är 100% vattentätt precis som det inte finns något dörrlås, brandvarnare eller Systembolag som är 100% vattentätt. Dörrlås kan brytas upp, brandvarnare kan gå sönder och det går att be en person över 18 år att köpa ut alkohol. Den som vill ta sig runt ett porrfilter kommer alltid kunna göra det, men samhället begränsar olika saker som är skadliga för barn så gott det går. Porrfilter/teknisk lösning har även ett viktigt **normbildande signalvärde**. Det finns olika porrfilter/tekniska lösningar som har mer eller mindre effekt, därför är det viktigt att **testa valt alternativ regelbundet** och att kombinera porrfilter/teknisk lösning med porrfri policy, åldersanpassad regelbunden porrkritisk undervisning och porrkritiska samtal. Kontakta Sveriges Kommuner och Regioner för vägledning om val av porrfilter/teknisk lösning.

Källor:
*https://polisen.se/siteassets/dokument/ovriga_rapporter/lagesbild-over-sexuella-ofredanden.pdf
**http://unizon.se/engagera-dig/resurser-och-material/10-sammanfattande-punkter-fran-forskningen-om-porr-och
***https://www.expressen.se/kultur/qs/sa-radikaliseras-man-av-valdsporren/
****Magdalena Mattebo, Uppsala universitet, 2016

Mer information:
Det här dokumentet är framtaget av barnrättsorganisationen Porrfri Barndom i november 2018. För mer information om barns ofrivilliga exponering för nätpornografi, barns porrkonsumtion och dess hälsokonsekvenser för barn samt referenser till ovan vänligen besök: https://www.porrfribarndom.se/

Rutin för informationssäkerhet medarbetare

Version 2.1	2020-04-24 Säkerhetsutvecklare
Antagen av kommundirektör	2020-09-17
Reviderad (videomöte)	2021-09-23 Säkerhetschef
Antagen av kommundirektör	2021-09-28

Rutin

beskriver ett arbetssätt för vad som ska göras, i vilken ordning och av vem.

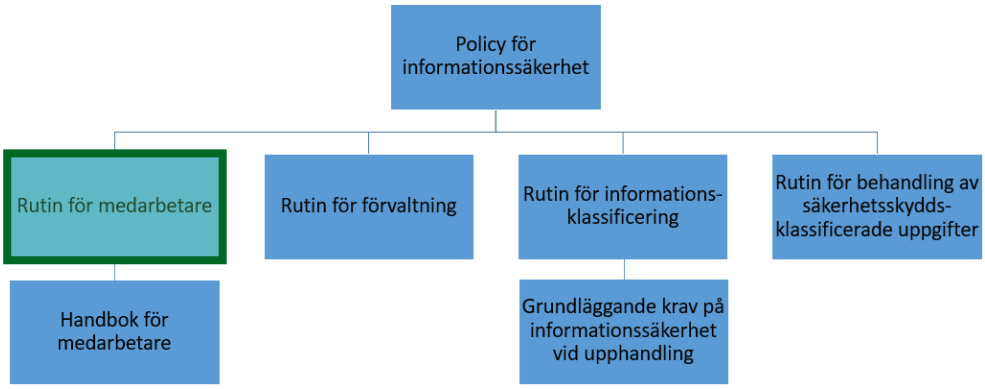
Innehållsförteckning

1. Inledning

Information är en viktig tillgång för Härryda kommun. Med informations-tillgångar avses all information oavsett om den behandlas manuellt eller automatiserat och oberoende av dess form (muntligt, skriftligt, digitalt etc.) eller miljö den förekommer i.

I Härryda kommuns hanteras stora mängder information. Du som anställd har ett ansvar att bidra till att informationen hanteras på ett säkert sätt.

Denna *Rutin för informationssäkerhet medarbetare* är en konkretisering av *Policy för informationssäkerhet* och ska ge dig stöd att upprätthålla god säkerhet när du hanterar olika typer av informationstillgångar i ditt arbete. Rutinbeskrivningen innehåller grundläggande anvisningar och riktlinjer för hur information förväntas att hanteras i kommunen.



Figur 1: Kommunens styrdokument för informationssäkerhetsarbetet. Grön färgmärkning anger det aktuella dokumentet.

1.2 Ansvarsfördelning

Ansvaret för genomförandet i enlighet med styrdokumentationen för kommunens arbete med informationssäkerhet följer linjeorganisationen.

Samtliga medarbetare ansvarar för att efterleva kommunens policy och rutiner framtagna för informationssäkerhetsarbetet.

Om du har frågor om informationssäkerhetsarbetet vänder du dig i första hand till din chef.

1.3 Avgränsningar

Det finns en *Handbok för informationssäkerhet medarbetare* tillgänglig på IDA som är mer detaljerad och utförlig i vissa avseenden. Hänvisning till handboken sker med stöd av fotnotsmarkeringar för respektive kapitel eller avsnitt som är aktuellt för ändamålet.

2. Åtkomst till information

Kommunens informationssystem är utrustade med behörighetskontrollsystem för att säkerställa att endast behöriga medarbetare kommer åt informationen.

2.1 Behörighet

Alla medarbetare i Härryda kommun ska ha personliga inloggningsuppgifter för åtkomst till kommunens nätverk och IT-stöd.
Detta innebär att du inte får lämna ut dina inloggningsuppgifter till någon annan. Du får inte heller nyttja någon annans konto.
Dina arbetsuppgifter styr vilka behörigheter du blir tilldelad. Behörigheter beslutas av din chef/systemägare.

2.2 Inloggning

Innan du loggar in första gången får du ett lösenord av Servicedesk eller av din chef för åtkomst till kommunens interna IT-nätverk. Lösenordet ska du byta till ett personligt lösenord efter första inloggningen. För enskilda program och system som kräver lösenord kontaktar du respektive systemförvaltare/systemadministratör.

2.3 När du är inloggad och uppsikt över utrustning[1]

När du loggat in ska du tänka på att aldrig lämna din digitala utrustning (dator, läsplatta, mobiltelefon) obevakad. De flesta verksamhetssystem innehåller funktioner för spårbarhet. Om någon annan person ”lånar” din inloggade dator är du ansvarig för de handlingar som utförs med ditt konto.
Vid de tillfällen du inte har uppsikt över din digitala utrustning ska du förhindra att andra kan använda din utrustning.

2.4 Distansarbete[2]

För att på ett säkert sätt få åtkomst till flertalet utav kommunens verksamhetssystem måste du använda en så kallad VPN-uppkoppling[3] när du arbetar på distans. Webbaserade applikationer som t.ex. Office 365 nås genom att endast ansluta din arbetsdator till Internet.

Du ska vara uppmärksam på vilken information du delar med dig av vid telefonsamtal eller som syns på skärmen vid distansarbete eftersom obehöriga inte ska ha möjlighet att ta del av informationen.
Dina digitala arbetsverktyg får inte användas av familjemedlemmar eller andra obehöriga användare.

---

[1] Handbok för informationssäkerhet medarbetare
[2] Handbok för informationssäkerhet medarbetare
[3] Virtuellt privat nätverk (VPN) (engelska: *Virtual Private Network*) är en teknik som används för att skapa en säker förbindelse eller "tunnel" mellan två punkter i ett icke-säkert datanätverk (till exempel Internet). Härryda kommun använder Cisco AnyConnect Secure Mobility Client för detta ändamål.

Digitala arbetsverktyg är stöldbegärliga och det är därför viktigt att du inte ställer ifrån dig utrustningen obevakad. Utrustningen ska alltid vara lösenordskyddad.

2.5 Hantering av lösenord[4]

Ditt användarkonto är personligt och därför krävs lösenord för att använda det. Ett lösenord ska:

- vara minst åtta tecken långt
- bestå av en blandning av stora & små bokstäver/siffror/specialtecken
- inte innehålla ditt namn och/eller efternamn
- inte vara detsamma som ditt kontonamn
- inte återanvändas

Byte av lösenord är aktuellt:

- var 60:e dag när det gäller interna nätverket. Du får en påminnelse via mail innan lösenordet går ut
- för enskilda program och system efter ett visst tidsintervall som bestäms av respektive systemägare
- omedelbart om du misstänker att någon annan känner till ditt lösenord

3. Digital utrustning och applikationer

3.1 Utrustning

IT-funktionen levererar överenskomna digital utrustning[5] som ska och får nyttjas inom kommunen. Detta innefattar all hårdvara såsom datorer, surfplattor, telefoner samt kringutrustning. För den utrustning som du förfogar över, exempelvis dator och läsplatta, gäller:

- Vid eventuella fel på din digitala utrustning ska du omgående anmäla detta till Servicedesk.
- Fysiska ingrepp får endast utföras av IT-funktionen eller leverantör.

3.2 Kassering av utrustning

Vid behov av kassering av digital utrustning som exempelvis dator, telefon, läsplatta etc. ska lämnas till Servicedesk.

3.3 Applikationer

För applikationer och programvaror gäller följande:

- Applikationer för privat bruk får inte installeras och användas på kommunens arbetsdatorer.

---

[4] Handbok för informationssäkerhet medarbetare

[5] För personal inom sektor UTK gäller detta endast den utrustning som leasas.

- Det är inte tillåtet att kopiera eller använda Härryda kommuns applikationer eller verksamhetssystem på privat utrustning.

4. Hantering och lagring av information

4.1 Hantering av information

Du som medarbetare hanterar dagligen olika typer av information såväl muntligen som i skrift, digitalt och i pappersform. Det är viktigt att du har kännedom om hur olika typer av information ska hanteras.

4.1.1 Allmänna handlingar

I ditt arbete hanterar du allmänna handlingar, dessa kan vara offentliga eller sekretessbelagda. Det är viktigt att du känner till skillnaden. För mer information se kommunens ärendehanteringsbok. Alternativt kontakta din sektors administrativa chef/administratör.

4.1.2 Sekretesshandlingar

Sekretesshandlingar är hemliga och det innebär en begränsning i rätten att ta del av dem för allmänheten eller annan obehörig inom förvaltningen. Om du hanterar sekretesshandlingar behöver du tänka på att sekretessbelagda handlingar i pappersformat aldrig får förvaras oskyddade eller lämna arbetsplatsen.

Sekretesshandlingar ska förvaras i ett godkänt säkerhetsklassat skåp. Verksamhetschef/enhetschef ansvarar för samordning och inköp av skåp. Säkerhetsfunktionen i kommunen ska förmedla kontakt vid inköp samt stöd med bedömning av verksamhetens behov.

4.1.3 Personuppgifter

Personuppgifter ska hanteras varsamt. Du behöver därför känna till grunderna i Dataskyddsförordningen (GDPR) som främst syftar till att skydda hanteringen av personuppgifter. Förvaltningen har därför tagit fram en GDPR-handbok som finns tillgänglig på IDA.
Alternativt kontakta din sektors administrativa chef/administratör.

4.1.4 Datamedia

Digital utrustning/datamedia som ska avvecklas och som innehåller datamedia med sekretessbelagd information överlämnas till Servicedesk som hanterar avvecklingen.

4.2 Lagring av information

Övergripande gäller att all information som du skapar alltid ska lagras på kommunens centrala lagringsutrymme.
Lagring av information som är av privat karaktär är inte tillåten.

4.2.1 Verksamhetssystem

I första hand ska sekretessklassad information och *känsliga eller extra skyddsvärda personuppgifter*[6] alltid lagras i respektive verksamhetssystem.

Om det saknas verksamhetssystem för den information du producerar, finns följande alternativ för lagring av information enligt nedan.

4.2.2 Office 365[7]

Observera att sekretessklassad information enligt lag samt *känsliga eller extra skyddsvärda personuppgifter* inte får lagras i Office 365 och dess applikationer.

Teams
Här kan du hantera samt lagra arbetsmaterial som flera behöver ha tillgång till.

Onedrive
Här kan du hantera samt lagra eget arbetsmaterial.

Outlook
Epostsystemet är en viktig informationskanal men inget arkiv.
Mer information om hur du ska hantera din e-post finns i förvaltningens Policy för hantering av e-post.

4.2.3 Lagring på disk

O:/ -katalog
Här lagrar du sekretessklassad information enligt lag samt *känsliga eller- extra skyddsvärda personuppgifter* som flera behöver ha tillgång till, om du inte har tillgång till ett verksamhetssystem. Respektive sektor har sin egen mappstruktur. Kontakta din chef för att ta reda på vad som gäller för din verksamhet.

H:/ -katalog
Här lagrar du arbetsmaterial som bara du ska ha tillgång till och som är sekretessklassad information enligt lag samt *känsliga- eller extra skyddsvärda personuppgifter*. Detta gäller om du inte har tillgång till ett verksamhetssystem.

---

[6] GDPR-handboken på IDA innehåller en beskrivning av aktuella definitioner.
[7] Handbok för informationssäkerhet medarbetare

Hårddisk C:
Hårddisk C: eller skrivbordet på datorn ska inte användas för lagring av någon typ av information.

Lagringsmedier
När du lagrar data på USB eller andra externa lagringsmedia är det av största vikt att du har kontroll över detta. Du ska vara återhållsam med att använda externa lagringsmedia eftersom de lätt kan tappas bort och känslig information därmed kan hamna i orätta händer.

Om sekretesskyddad information enligt lag, *känsliga- eller extra skyddsvärda personuppgifter* lagras på extern lagringsmedia måste dessa förvaras inlåsta i ett godkänt säkerhetsskåp för ändamålet. Säkerhetsfunktionen i kommunen ska förmedla kontakt vid inköp av säkerhetsskåp.

4.2.4 Säkerhetskopiering
Alla lagringsplatser som nämnts ovan, förutom hårddisk C:, säkerhetskopieras automatiskt. Säkerhetskopian sparas i 30 dagar.

4.3 Utskrift av dokument
Vid utskrift av dokument via nätverksskrivare är det *secure-print* funktionen som gäller. Om du måste skriva ut information som kan bedömas som *känsliga eller extra skyddsvärda personuppgifter* eller är sekretessbelagd enligt lag, krävs en särskild riskbedömning.

4.4 Videomöte
Teams ska användas för videomöten även av verksamheter inom exempelvis socialttjänst och skola. Om bedömningen görs att extra känslig information ska delas under mötet ska andra mötesformer övervägas som till exempel fysiskt möte eller telefon.

Om Teams videomöte används för möten där sekretess föreligger ska följande åtgärder vidtas:

- Använd lobbyfunktionen för att säkerställa vilka som deltar i mötet.
- Säkerställ genom uppvisande av legitimation att deltagarna på mötet är den de utger sig för att vara.
- Sitt på en plats där ingen obehörig kan ta del av det som sägs under mötet, använd gärna headset.
- Mötet får inte spelas in.
- Möteschatten får inte användas.
- Dela inte dokument på skärmen.
- Andra appar som exempelvis Facetime får inte användas.

5. Incidenthantering- och rapportering[8]

Varje verksamhet i kommunen ansvarar för att anmälan av en informationssäkerhetsincident görs enligt nedan, samt för att utreda och vidta eventuella åtgärder med anledning av en inträffad incident. Ansvaret för incidenthantering och rapportering följer därmed linjeorganisationen. Vid behov av stöd och råd kan kommunens säkerhetsutvecklare konsulteras.

5.1 Incidenthantering

5.1.1 Vad är en informationssäkerhetsincident?

Med informationssäkerhetsincident menas en oönskad händelse som påverkar, eller kan komma att påverka, kommunens informationstillgångar negativt.

En incident kan antingen bero på ett avsiktligt eller ett oavsiktligt agerande. Den gemensamma nämnaren är att informationssäkerheten hotas, det vill säga, att händelsen kan utgöra ett hot mot att informationen inte uppfyller kraven vad gäller *tillgänglighet, riktighet, sekretess* och *spårbarhet*[9].

I sammanhanget informationssäkerhet kan detta exempelvis vara:

- information (ex. dokument/filer) hamnar på avvägar/förloras
- din arbetsdator/verksamhetssystem utsätts för intrångsförsök
- du mottar eller misstänker falsk e-post (s.k. ”phishing”)

5.1.2 Vad är en personuppgiftsincident?

En *personuppgift*[10] är all slags information som direkt eller indirekt kan knytas- och användas för att identifiera en person.

En personuppgiftsincident är en händelse som leder till att personuppgifter förloras, uppdateras felaktigt, förstörs eller kommer i orätta händer (obehöriga tar del av). Det spelar ingen roll om händelsen inträffat oavsiktligt eller med avsikt. I båda fallen är det personuppgiftsincidenter.

För mer information angående vad som gäller vid behandling av personuppgifter enligt Dataskyddsförordningen (GDPR) kan du läsa mer på kommunens intranät IDA. Alternativt kan du kontakta din sektors administrativa chef.

---

[8] Handbok för informationssäkerhet medarbetare

[9] *Tillgänglighet* -att information och informationstillgångar kan utnyttjas efter behov, i förväntad utsträckning och inom önskad tid. *Riktighet* -informationen ska vara tillförlitlig, korrekt och fullständig. *Sekretess* -att innehållet i dokument, information och handlingar inte görs tillgängliga eller avslöjas för obehörig. *Spårbarhet* -det ska gå att se vem som tagit del av informationen, vilka förändringar som har skett och av vem dessa har utförts.

[10] Exempel på *personuppgifter* är: namn, personnummer, adress och telefonnummer, foton, filmer och ljudupptagningar där det tydligt går att identifiera en person, en fastighetsbeteckning, en besökares IP-adress på en hemsida, om den är en del av annan data.

5.1.3 Vad är skillnaden mellan en informationssäkerhets- och en personuppgiftsincident?

Skillnaden mellan en informationssäkerhetsincident och en personuppgiftsincident, är att det sistnämnda fokuserar på hantering av personuppgifter som behandlas i en informationstillgång. Behandling av personuppgifter enligt Dataskyddsförordningen (GDPR) utgör därför ett delområde underordnad arbetet med informationssäkerhet i kommunen.

5.2 Rapportering av incidenter inom förvaltningen

Det är av yttersta vikt att samtliga informationssäkerhetsincidenter rapporteras omgående. En grundregel som är tillämpbar vid anmälan av en incident, är att utgå från om det inträffade berör personuppgifter enligt Dataskyddsförordningen (GDPR). Om svaret på den frågan är ja, så anmäls händelsen som en personuppgiftsincident och inget annat. Incidenter som inte faller inom ramen för Dataskyddsförordningen men utgör ett hot mot informationssäkerheten, ska incidenten anmälas som en informationssäkerhetsincident. Den som ansvarar för att anmälan av en incident upprättas, förväntas alltså inte att göra två separata anmälningar.

5.2.1 Rutin för rapportering av informationssäkerhetsincidenter

Informationssäkerhetsincidenter ska rapporteras till närmsta chef, eller systemförvaltare/systemadministratör för det aktuella IT-systemet där incidenten ägt rum. Ovannämnda funktioner ansvarar för att göra anmälan via e-tjänsten anmäla informationssäkerhetsincident på IDA.

Ovannämnda funktioner ska göra en kompletterande anmälan till Servicedesk om incidenten påverkat IT-utrustning och data- eller telekommunikation. Vid fråga om stöld ska en kompletterande polisanmälan upprättas av ovannämnda funktioner.

5.2.2 Rutin för rapportering av personuppgiftsincidenter

Personuppgiftsincidenter rapporteras när du:

- vet att det har inträffat en incident
- misstänker att det har inträffat en incident
- ser en risk för att det kan inträffa en incident

Alla personuppgiftsincidenter ska rapporteras så snart som möjligt.
Det gäller även om incidenten hunnit bli åtgärdad.

Om du upptäcker en personuppgiftsincident ansvarar du för att omgående rapportera samt meddela din närmaste chef. Anmälan av personuppgiftsincident sker på kommunens intranät IDA.

5.2.3 NIS-direktivet

Enligt föreskrifter från *Myndigheten för Samhällsskydd och Beredskap (MSB)* [11] ska kommunen rapportera incidenter som orsakar *störningar*[12] som får betydande inverkan på kontinuiteten i den samhällsviktiga tjänsten. Berörda verksamheter i kommunen ansvarar för att bedöma om den egna verksamheten omfattas av föreskriften och att rapportering av incidenter sker i enlighet med gällande anvisningar.

Vid behov av stöd och råd kan kommunens säkerhetsutvecklare konsulteras.

[11] MSBFS 2018:9 Föreskrifter och allmänna råd om rapportering av incidenter för leverantörer av samhällsviktiga tjänster

[12] Med störning i den samhällsviktiga tjänsten menas en konsekvens av en incident som innebär att den samhällsviktiga tjänsten inte levereras som normalt.

6. Personalsäkerhet[13]

6.1 Före- och i samband med anställning

Bakgrundskontroll av sökande (gäller även leverantörer) till tjänster i Härryda kommun ska ske genom verifiering av meritförteckning.

Registerkontroll ska även utföras vid anställning av personal/leverantör när detta krävs av lag eller författning.

Bedömning/klassificering av vilken behörighet och tillgång till information medarbetaren/leverantören ska ha i proportion till gällande verksamhetskrav och tilltänkta arbetsuppgifter.

Nyanställda/leverantörer ska ta del kommunens styrdokumentation för informationssäkerhetsarbetet, de delar av styrdokumentationen som är relevanta för den specifika medarbetaren/leverantören. Det är viktigt att ansvar och skyldigheter kring informationssäkerhet delges berörda.

I de fall som det krävs av lag eller författning, ska anställda/externa aktörer/leverantörer som får tillgång till konfidentiell information underteckna ett avtal om tystnadsplikt/sekretess[14]. Ansvaret enligt avtal bör även gälla efter att anställningen är avslutad.

6.2 Under anställning

Alla medarbetare, leverantörer och i förekommande fall externa aktörer ska erhålla lämplig utbildning för att kunna efterleva kommunens policy och rutiner för informationssäkerhet.

Om anställda/leverantörer bryter mot gällande informationssäkerhetsregler ska dessa ärenden hanteras individuellt av ansvarig chef med stöd av personalfunktionen på samma sätt som vid annan misskötsel.

6.3 Vid avslut- eller ändrad anställning

Vid avslut eller ändring av anställning kan ansvar och skyldigheter kring sekretess och tystnadsplikt fortsätta vara gällande om medarbetaren/leverantören haft tillgång till konfidentiell information. Ett sekretessavtal ska upprättas i de fall som det krävs av lag eller författning. Detta ska kommuniceras till den anställde/leverantören när denne påbörjar, förändrar och avslutar sin anställning.

- Återlämnande av digital utrustning och indrag av åtkomsträttigheter till information ska ske i direkt samband med avslut- eller ändring av anställning.
- Allt arbetsmaterial du framställer är Härryda kommuns egendom och får inte tas med utan godkännande av din chef.
- De behörigheter du fått för åtkomst till kommunens informationssystem avbeställs av din chef.

[13] Handbok för informationssäkerhet medarbetare
[14] Mall för avtal om tystnadsplikt/sekretess på IDA

- Rådgör med din chef om vilket av ditt arbetsmaterial som ska sparas och i förekommande fall vidarebefordras till lämplig(a) person(er). Ta bort resterande information.
- Lämna tillbaka all utrustning som tillhör Härryda kommun till din chef.

7. Internet[15]

När du surfar på internet representerar du Härryda kommun och lämnar spår efter dig i form av Härryda kommuns IP-adress.

Det är inte tillåtet att via internet ta del av eller publicera material av pornografisk-, rasistisk-, eller förtroendeskadlig karaktär. Förbudet gäller också material som är diskriminerande eller har anknytning till kriminell verksamhet eller på annat sätt oförenligt med svensk lagstiftning.

Du ska också vara medveten om att det är otillåtet att, utan upphovsmannens medgivande, kopiera eller på annat vis använda material som finns på internet. Med material avses exempelvis bilder, fotografier, texter, musik och datorprogram.

8. Sociala medier

Det är ansvarig chef som beslutar om och hur verksamheten ska använda sig av sociala medier i sin kommunikation. Det innebär att det måste finnas ett uppdrag från chefen för att en medarbetare ska kunna använda sociala medier i tjänsten. Ansvarig chef anmäler sida/blogg/konto och vem på enheten/verksamheten som ska sköta den. Anmälan skickas till kommunikationsenheten. Mer information om anmälan och blanketter finns på kommunens intranät IDA.

Tänk på att du använder sociala medier som anställd i Härryda kommun och inte som privatperson.

[15] Handbok för informationssäkerhet medarbetare