Piteå kommun

Anvisning för säkerhetsskyddsklassificerade uppgifter i fristående dator

Dokumentnamn	Dokumenttyp	Senast reviderad	Beslutsinstans
Anvisning för säkerhetsskyddsklassificerade uppgifter i fristående dator	Anvisning	2020-08-21	Kommunchef
Dokumentansvarig/processägare	**Version**	**Diarienummer**	**Giltig till**
Kommunledningsförvaltningen	1	20KS377	2024-12-31
Dokumentinformation	Säkerhetsinstruktioner		
Dokumentet gäller för	Anställda inom Piteå kommun		

1. Definitioner

Fristående IT-systemet	Den datorutrustning som behövs för behandling av digitala säkerhetsskyddsklassificerade uppgifter. Det innefattar: • fristående dator (härdad dator) • CD-ROM brännare • extern lagringsmedia • skrivare • tvättmaskin
Fristående dator	En dator som är nedlåst säkerhetsmässigt, dvs. härdad mot intrång och obehörig åtkomst av information från omvärlden och som innehåller säkerhetsskyddsklassificerade uppgifter.
CD-ROM brännare	Används för säkerhetskopiering av den fristående datorn.
Extern lagringsmedia	USB-minne, CD-ROMskiva, USB-hårddisk
Fristående skrivare	En skrivare utan nätverksstöd och trådlösöverföring samt lagringsmedia, anpassad för att hantera utskrifter av säkerhetsskyddsklassificerade uppgifter.
Tvättmaskin	En dator som har minst två olika typer av antivirusprogram som kan utföra grundlig genomlysning efter skadlig kod på extern lagringsmedia.
Skyddsvärd information	Säkerhetsklassad information, utifrån både kommunens och Sveriges säkerhet.
Säkerhetsskyddsklassificerade uppgifter	Information klassificerad utifrån Sveriges säkerhet.
Säkerhetsskyddsanalys	Identifiera hotbild och vilka skyddsvärda tillgångar kommunen har utifrån Sveriges säkerhet.

2. Allmänt

För att kunna säkerställa att verksamheten har det skydd som behövs för sina digitala informationstillgångar krävs det att man har gjort en säkerhetsskyddsanalys på de skyddsvärda informationstillgångarna, främst på förekomsten av säkerhetsskyddsklassificerade uppgifter. Utifrån vad som framkommit i säkerhetsskyddsanalysen kan verksamheten sedan applicera adekvata säkerhetsåtgärder avseende informationssäkerhet, tillträdesbegränsning och säkerhetsprövning av personal.

För att få ta del av och arbeta med hemlig uppgift i fristående datorer (s.k. H-dator, anpassad för hantering av säkerhetsskyddsklassificerade uppgifter), ska personalen genomgå en säkerhetsprövning och placeras i säkerhetsklass som motsvarar den klassificering som den hemliga uppgiften är placerad i.

För att veta vilken skyddsnivå den digitala informationen ska ha, behöver skyddsvärd information värderas och klassas enligt MSB:s verktyg KLASSA. Uppgifter med högre skyddskrav kan inte klassificeras med KLASSA utan måste värderas enligt den klassificeringsnivåer som är fastställd enligt säkerhetsskyddslagstiftningen[1].

- KVALIFICERAT HEMLIG - vid en synnerligen allvarlig skada
- HEMLIG - vid en allvarlig skada
- KONFIDENTIELL - vid en inte obetydlig skada
- BEGRÄNSAT HEMLIG - vid endast ringa skada.

Klassningen styr vilka säkerhetsåtgärder som måste vidtas avseende valet av IT-utrustning och hur de säkerhetsskyddsklassificerade uppgifterna behandlas och förvaras.

Den samlade mängden av skyddsvärd information, dvs. den aggregerade mängden information, kan även innebära att uppgifterna får ett högre skyddsvärde än den enskilda uppgiften.

3. Behandling av säkerhetsskyddsklassificerade uppgifter i fristående dator

3.1. Fristående dator

Datorn ska vara härdad och anpassad för att endast användas för fristående bruk. Det innebär att den inte kan anslutas till nätverk av något slag, vare sig det handlar om trådbunden eller trådlös kommunikation. Lagringsmedia kan inte heller avläsas då det är krypterat. All kommunikationsmöjlighet är bortplockat ur datorn och alla portar och luckor är förseglade utom en USB-port för att möjliggöra avläsning, utskrifter och systemuppdatering samt VGA/HDMI för presentation av material via projektor.

Om någon försegling skulle bli bruten, ska den hemliga informationen anses röjd och händelsen incidentrapporteras till tillsynsmyndighet.

[1] Säkerhetsskyddslagen SFS 2018:585

Datorn är anpassad för en användare och får således inte nyttjas av annan personal än den är avsedd för. Ska flera personer använda samma dator måste dessa inneha samma säkerhetsklass och vara godkända att ta del av den hemliga information datorn innehåller.

Datorn uppfyller säkerhetsklassificering Begränsat hemlig och får således inte innehålla eller användas för behandling av hemlig information klassificerad på högre nivåer.

3.2. Användarkonto

Den fristående datorn innehåller användarkonto som ska användas av den person som kontot är tilldelat till. Användaren får således inte låna ut sina kontouppgifter till annan användare. Användaren måste logga ut innan annan personal får nyttja datorn. Det är av största vikt att användaren skyddar sina kontouppgifter så att ingen får tillgång till dem.

Det finns även ett Administratörskonto och det får endast användas för systemunderhåll av systemansvarig och behörig supportpersonal. Observera att supportpersonal måste genomgått en säkerhetsprövning och inneha samma säkerhetsklass som systemansvarig och användare av den fristående datorn.

Alla inloggningsuppgifter ska vara dokumenterade och förvaras i förseglat emballage dvs. säkerhetspåse och förvaras i godkänt säkerhetsskåp[2] för hemliga handlingar.

3.3. Lokaler

Vid behandling av säkerhetsskyddsklassificerade uppgifter är man tvungen att uppfylla särskilda krav som minimerar avlyssning av både lokaliteter och teknisk utrustning.

Lokalen där säkerhetsskyddsklassificerade uppgifter behandlas bör vara ordnad på så sätt att riskerna minimeras så långt det är möjligt för akustisk avlyssning, dvs. det ska inte gå att avlyssna vad som sägs genom väggar, golv, dörrar, fönster, ventilationssystem eller övriga kanalisationer. Lokalen bör heller inte innehålla några former av elektronisk utrustning kopplade till datornätverk eller trådlösa nätverk, t.ex. mobilnät, wifi osv. Personal som ska delta blir således tvungen att lämna ifrån sig personlig IT-utrustning så som datorer, surfplattor, mobiltelefoner, smarta klockor osv.

Avser man behandla uppgifter med säkerhetsklassificering högre än Begränsat hemlig måste lokalen vara RÖS-skyddad (skydd mot röjande signaler), om ingen tillgång till RÖS-skyddad lokal finns måste fristående datorn vara RÖS-skyddad.

3.4. Överföring

Vid överföring av digitala säkerhetsskyddsklassificerade uppgifter krävs det nationellt godkända kryptolösningar, dessa kan endast tillhandahållas av FRA[3] och särskilda krav på signalskydd måste uppfyllas innan så kan ske. Detta för att säkerställa att säkerhetsskyddsklassificerade uppgifter inte förvanskas eller röjs till obehöriga elektroniskt vid överföring.

[2] Säkerhetsklass SSF 3492
[3] Försvarets radioanstalt

3.5. Medförande

Medförande innebär när en person i sin tjänst behöver transportera och förvara en fristående dator eller lagringsmedia utanför verksamhetens område och lokaler. Man bör också beakta det ökade skyddsvärdet på den fristående datorn eller lagringsmediet utifrån den aggregerade information som den innehåller.

Medförande av digitala säkerhetsskyddsklassificerade uppgifter och dess tekniska utrustning där dessa finns lagrade innebär att man riskerar att uppgifterna kan röjas till obehörig. För att undvika detta ska säkerhetsskyddsklassificerade uppgifter inte medföras om så inte är synnerligen nödvändigt.

Om medförande måste ske så ska den fristående datorn eller lagringsmediet innehållande säkerhetsskyddsklassificerade uppgifter, alltid hållas under omedelbar uppsikt och förvaras enligt samma skyddsnivå som i den egna verksamhetens lokaler.

Det är även viktigt att:

- Säkerhetskopiering eller dokumentation har utförts på datorns eller lagringsmediets innehåll
- När datorn eller lagringsmediet inte används ska dessa förvaras i förseglat emballage under medförandet, förslagsvis en säkerhetspåse, detta för att ett eventuellt intrång ska kunna försvåras och därmed uppmärksammas.

Regler för medförande finns reglerade i anvisning för administration av säkerhetsskyddklassificerade handlingar.

4. Systemunderhåll

Systemunderhåll utförs när behov uppstår. Uppdateringar av operativsystem eller dess applikationer ska ske genom verksamheten godkända säkerhetsuppdateringar. För att en uppdatering ska kunna föras in i en fristående dator måste följande steg beaktas:

- Säkerhetskopiering av den fristående datorn ska utföras innan systemunderhåll påbörjas.
- Filerna för uppdatering ska placeras på ett godkänt och dedikerat USB-minne och tvättas i en så kallad ”tvättmaskin”[4].
- Därefter kan USB-minnet användas för att uppdatera den fristående datorn.
- Efter uppdatering ska lagringsmediet förstöras som säkerhetsåtgärd för att förhindra att säkerhetsskyddsklassificerade uppgifter förts över till USB-minnet som obehöriga senare kan komma åt.

[4] En dator som har minst två olika typer av antivirusprogram som kan utföra grundlig genomlysning efter skadlig kod på extern lagringsmedia.

5. Systemförvaltning

5.1. Systemägare

Systemägare är verksamhetschef för den verksamhet som har behov av att nyttja det fristående IT-systemet för behandling och förvaring av digitala säkerhetsskyddsklassificerade uppgifter i sin verksamhet. Systemägaren ansvarar för att se till att verksamheten har de nödvändiga resurser som krävs för att förvalta och underhålla fristående IT-systemet under hela levandscykeln.

5.2. Systemansvarig

För att vara systemansvarig så måste personen genomgått en säkerhetsprövning och vara placerad i säkerhetsskyddsklass. Det är viktigt att personen i fråga får en god uppfattning av vilka krav som ställs på det fristående IT-utrustningen för att behandla säkerhetsskyddsklassificerade uppgifter. Systemansvarig är den som ansvarar för att sköta om att administration, drift och systemsupport upprätthålls samt efterlevnaden av de säkerhetsåtgärder som ställs efterlevs. Systemansvarig är även den som har kontakt med leverantör och systemtekniker när så krävs.

5.3. Systemsupport

Innan den fristående IT-utrustningen får hanteras av en systemtekniker måste denne genomgått säkerhetsprövning och placerats i säkerhetsskyddsklass. Det är viktigt att personen i fråga får en god uppfattning av vilka krav som ställs på det fristående IT-systemet för att behandla säkerhetsskyddsklassificerade uppgifter. Detta då systemtekniker även får administrationsrättigheter och därmed skulle kunna förändra inställningar som försämrar skyddet av datorn.

Lokalen där konfiguration och systemunderhåll ska ske, måste vara tillträdesbegränsad så att det endast medger inpassering av säkerhetsskyddsklassificerad personal och som i sitt tjänsteutövande har behov av att vistas och arbeta i lokalen. Utöver det ska lokalen ha adekvata säkerhetsskyddsåtgärder som förhindrar intrång och stöld utifrån säkerhetsskyddsklassificering på de uppgifter som finns i lokalerna. När arbete inte sker på den skyddsvärda utrustningen, ska denna låsas in i för ändamålet godkänt säkerhetsskåp.

5.4. Användare

För att få tillgång till fristående IT-dator ska personen ifråga först genomgått säkerhetsprövning och vara placerad i säkerhetsskyddsklass. Denne ska även fått till sig instruktioner för hur den fristående datorn får användas och vilka rutiner som gäller, därefter skriftligen kvittera ut utrustningen man blivit tilldelad. Ska datorn lagras i ett säkerhetsskåp där andra förvarar sin utrustning, måste användaren skriva på ett samförvaringsbeslut och i det aktuella säkerhetsskåpet ska det finnas låsbara fack där var och en förvarar sin fristående dator var för sig.

6. Lagringsmedia

Lagringsmedia kan vara USB-minne eller en USB-hårddisk men även information lagrad på en CD-skiva. Då denna typ av lagringsmedia är små fysiskt men kan innehålla stora mängder

information och lät kan tappas bort, innebär det att vid förlust kan det medföra stora konsekvenser ifall informationen blir röjd.

Principen är därför att vi ska undvika användningen av denna typ av lagringsmedia så långt det är möjligt.

7. Säkerhetskopiering

För att säkerställa att den information som lagras i fristående dator inte försvinner ifall datorn går sönder eller att den inbyggda hårddisken kraschar ås är det av största vikt att regelbundet ta säkerhetskopia på alla dokument som lagras i datorn.

Säkerhetskopiering ska utföras innan systemuppdateringar ska installeras, eller när man skapat eller reviderat större mängd information,

Minimum är att alltid ta en säkerhetskopia av den lagrade informationen 1 gång var 6:e månad.

Brukas datorn minst 1 gång i månaden ska säkerhetskopiering ske var 3:e månad.

Används datorn minst en gång i veckan ska säkerhetskopiering ske månatligen.

Alla säkerhetskopior bränns ut på CD-ROM och ska lagras hos registrator i godkänt säkerhetsskåp. Det måste alltid finnas minst 2 säkerhetskopior bakåt i tiden, övriga gallras årligen i samband med inventering av säkerhetsskyddsklassificerad information.

8. Skrivare, kopiator, scanner och övriga tillbehör

Vanliga nätverksanslutna skrivare, kopiator, scanner eller multifunktionsapparater osv. får inte användas tillsammans med fristående datorer och säkerhetsskyddsklassificerade uppgifter. För detta ändamål måste dedikerad utrustning införskaffas som inte kan anslutas till någon form av trådbunden eller trådlös kommunikation. Utrustningen får endast anslutas trådbundet till avsedd utrustning med USB-sladd. Utrustningen får ej heller innehålla någon form av permanent lagringsmedia (Hårddisk/SSD) för mellanlagring. Utrustning med löstagbar hårddisk får användas under förutsättning att hårddisken förvaras i godkänt säkerhetsskåp då utrustningen inte används.

Kan man inte plocka ut de komponenter som möjliggör kommunikation via nätverk, Bluetooth, NFC eller liknande kommunikationssätt måste dessa funktioner stängas av mjukvarumässigt i utrustningen.

Utrustningens alla portar och luckor som ger access till systemkort eller möjlighet att ansluta USB-minnen RAM-minnen osv. ska plomberas med assuranstejp, även chassit ska plomberas så att ingen kan öppna utrustningen utan att det märks och påverka dess innehåll och konfiguration.

Kan man inte förvara utrustningen i ett säkerhetsskåp så ska rummet den förvaras i vara ett låst utrymme samt omfattas av behörighetskontroll vid passage, rummet försett med volymlarm kopplat till larmcentral för att förhindra att ej säkerhetsskyddsklassificerad personal och obehöriga ges tillträde till skrivaren.

Efter utrustningen använts ska den göras strömlös och vänta 30 sekunder innan den får lämnas utan uppsikt.

9. Märkning

I det fall en handling bedöms innehålla säkerhetsskyddsklassificerade uppgifter ska detta framgå genom att handlingen förses med en hemligbeteckning. Även en fristående dator och eventuellt lagringsmedia ska så långt det är möjligt märkas. Detta gäller både allmänna och icke allmänna handlingar då det anger vilket skydd informationen i handlingen kräver.

10. Destruktion

Destruktion av fristående dator, skrivare och övriga tillbehör så som extern lagringsmedia får endast ske av säkerhetsskyddklassificerad personal och ska alltid utföras av två personer samt dokumenteras och verifieras av båda personerna som närvarat vid destruktionen.

10.1. Fristående dator

Innan destruktion ska säkerhetskopia tas på den lagrade informationen, därefter plockas den inbyggda hårddisken ut. Därefter får destruktion endast ske genom mekanisk bearbetning så till den grad att inget går att återskapa av den fysiska disken. Lämpligen körs disken in i en metalltugg som tuggar upp disken i beståndsdelar.

RAM-minne monteras ut och destrueras antingen genom mekanisk bearbetning eller bränning, om så inte kan ske ska hela moderkort där RAM-kretsarna sitter destrueras.

Om sådant inte finns tillgängligt måste disken först avmagnetiseras och sedan för hand mekaniskt bearbetas genom att borras sönder, kapas sönder, smältas ner eller på annat lämpligt vis destrueras så att information inte på något sätt helt eller i delar kan återskapas.

För extern lagringsmedia så som USB-hårddisk eller USB-minne gäller samma procedur som för inbyggd hårddisk i fristående dator.

Övriga komponenter i den fristående datorn kan källsorteras på samma vis som med övrig IT-utrustning.

10.2. CD-skivor

Godkänd dokumentförstörare som även klarar CD-skivor kan användas under förutsättning att dokumentförstöraren uppnår rätt säkerhetsklass för det media som ska destrueras. I övrigt kan destruktion ske genom att bränna upp mediet på samma sätt som för pappershandlingar.

10.3. Skrivare, CD-ROM och övriga tillbehör

Montera ut ev. lagringsmedia (RAM/ROM minneskretsar från utrustningen och destruera på samma sätt som för fristående dator, antingen mekaniskt eller genom bränning/smältning. Övriga komponenter kan källsorteras som vanligt.

11. Incident

En incident kan handla om uppsåtliga eller oavsiktliga händelser som medför störningar avseende konfidentialitet, riktighet eller tillgänglighet. En incident kan exempelvis vara dataintrång, olovlig avlyssning, stöld, spridning av skadlig kod eller manipulation av utrustning, kablage och lagringsmedia. Det kan också vara hård- eller mjukvarufel som uppstår utan någon yttre påverkan eller medvetet försök till sabotage.

Alla incidenter med betydelse för säkerheten ska skyndsamt rapporteras till Säkerhetsskyddschef för uppföljning och åtgärd enligt rutiner för incidenthantering.

Är man osäker huruvida det handlar om en incident ska detta rådgöras med Säkerhetsskyddschefen.

Viktigt att beakta vid rapportering av incident är följande:

- Vilka personer är inblandade?
- Vad har hänt?
- När hände det?
- När upptäcktes det?
- Hur hände det?
- När inventerades handlingarna eller lagringsmedierna senast?
- Vem har haft tillgång till uppgifterna?
- Vad finns det som tyder på att uppgifterna inte är röjda?

Svaren på ovanstående frågor ligger som underlag för eventuella skyddsåtgärder för att förhindra ytterligare röjande och eliminera eller minska konsekvenserna av den röjda uppgiften. Skyddsåtgärder kan även behöva vidtas tidigt efter att röjandet har upptäckts.

12. Avveckling

Vid avveckling eller återlämnande av den fristående datorn ska användaren som nyttjat datorn få en kvittens på att datorn är återlämnad. Detta kan med fördel noteras på samma underlag som användes för att kvittera ut utrustningen.

13. Källförteckning

MSB:s Det nya totalförsvaret – En hjälp på vägen! Hantering av säkerhetsskyddsklassificerade uppgifter i fristående datorer. (Publikationsnummer: MSB1309, ISBN: 978-91-7383-891-7)

https://www.msb.se/sv/publikationer/det-nya-totalforsvaret--en-hjalp-pa-vagen--hantering-av-hemliga-uppgifter-i-en-fristaende-dator/