HEDEMORA KOMMUN	**STYRDOKUMENT**	Sida 1(64)
Skapad av: Säkerhetschef	Datum 2021-11-22	Diarienummer: KS178-003 003
	Giltighet fr o m: 2022-05-17	Senast reviderad: KS 2018-11-06, § 129 (2018-09-14)
Godkänt/antaget av: Kommunstyrelsen den 17 maj 2022 § 47		
Dokumentansvarig: Säkerhetschef		

Riktlinje för Informationssäkerhet och dataskydd

Dok. Kategori:	Riktlinje
Stadie:	Beslutad
Gallring:	Bevaras
Kort beskrivning:	Riktlinjen ska reglera informations- och dataskyddsarbetet i kommunen så att arbetet bedrivs effektivt och med god kvalitet. Den anger ramarna för handlingsutrymmet i informations- och dataskyddsfrågor.

Hedemora kommuns olika styrdokument

Organiserade styrdokument Visar tydligt roll och ansvarsfördelning. - Reglemente - Delegationsordning - Bolagsordning	**Aktiverande styrdokument** Visar vad kommunen vill förändra och uppnå. - Strategi - Mål och budget - Program - Ägardirektiv - Handlingsplan och övrig plan - Förvaltningarnas verksamhetsplan - Bolagens affärsplan - Aktivitetsplan
Normerande styrdokument Tydliggör kommunens förhållningssätt och arbetssätt. - Policy - Riktlinje - Rutin och vägledning	**Regler för dem som bor och verkar i Hedemora kommun** Tydliggör villkoren för kommunal service och vilka krav kommunen ställer på de som bor och verkar i kommunen. - Avgifter (inkl. taxor) - Regler (inkl. lokala föreskrifter och lokala ordningar

Mer information om de olika styrdokumenten finns i Hedemora kommuns riktllinje ”Riktlinjer för styrdokument”.

Globala målen – Agenda 2030

Mål 16 i Agenda 2030 *handlar om Fredliga och inkluderande samhällen. Fredliga samhällen och frihet från våld utgör både ett mål och ett medel för hållbar utveckling. En väl fungerande statsförvaltning med ansvarsfulla institutioner, transparens och rättsstatens principer har alla ett fundamentalt egenvärde. De utgör grund för god samhällsstyrning inklusive korruptionsbekämpning och är viktiga drivkrafter för utveckling. Alla människor är lika inför lagen och ska ha lika tillgång till rättvisa sant ska ha möjlighet att utöva inflytande och ansvarsutkrävande över beslutsfattare. God samhällsstyrning och rättsstatens principer är grundläggande mål och medel för utveckling. Begreppen demokrati och de mänskliga rättigheterna återfinns inte uttryckligen under mål 16. Dessa begrepp förekommer dock tydligt i den politiska deklarationen i 2030-agendan.*

Delmål i mål 16

16.10 Säkerställa allmän tillgång till information och skydda grundläggande friheter, i enlighet med nationell lagstiftning och internationella avtal.

Innehåll

RIKTLINJE FÖR INFORMATIONSSÄKERHET OCH DATASKYDD

antaget av kommunstyrelsen den 17 maj 2022 § 47.

Inledning

Hedemora kommuns Informationssäkerhetspolicy och dataskyddsstrategi är övergripande dokument som redovisar kommunens övergripande mål och inriktning med informationssäkerhets- och dataskyddsarbetet.

Denna riktlinje – Riktlinje för informationssäkerhet och dataskydd – konkretiserar informationssäkerhetspolicyn och dataskyddsstrategin med mer detaljerad information och regler för hur information får hanteras inom kommunen.

Tillräcklig informationssäkerhet och ett gott dataskydd vid all informationshantering – en förutsättning för digitalisering.

Sedan ett par decennier befinner vi oss i en ny värld som innebär ett nytt paradigmskifte som kräver en stärkt informationshantering, informationssäkerhetsskydd och integritetsskydd för enskilda personer. En samhällsutveckling som vi idag kallar digitalisering. Persondata är nu det nya guldet och oljan i samhället. Hantering av känslig information och personuppgifter bygger på tillit och förtroende. Den offentliga förvaltningen ska vara innovativ, samverkande effektiv och rättssäker. Den ska ha en väl utvecklad kvalitet, service och tillgänglighet och på så sätt bidra till en god och säker samhällsservice och välfärd för invånarna.

Möjligheterna är enorma med digitaliseringen och den alltmer utbredda användningen av internet, som skapar helt nya möjligheter att utföra tjänster och dela information. Privatpersoner kan utföra en mängd digitala tjänster via internet (e-tjänster) från hemmet som bankärenden, kommunala tjänster, inköp, deklaration, bokningar, omröstning osv, och denna utveckling har lett till att de flesta idag förväntar sig att myndigheter, företag och andra organisationer ska erbjuda digitala tjänster på internet.

Det är inte bara traditionella datorer som är uppkopplade utan dessutom håller miljontals olika prylar – allt från kameror till bilar – att bli uppkopplade mot internet (”Internet of things”). Digitaliseringen ses som en möjliggörare och motor för en utveckling som innebär helt nya förutsättningar för samhället och människan. Hur det se ut om ytterligare tjugo år är svårt att föreställa sig och omöjligt att veta; idag går utvecklingen mycket snabbt mot något vi bara sett en början på.

Säkert är att det för kommunal verksamhet innebär stora förändringar inom de flesta områden. Nya företeelser som e-hälsa, e-förvaltning, e-demokrati, intelligenta transportsystem och smarta städer införs och digitalisering är redan något mycket mer och samhällsomfattande än bara kommuners IT-drift. Denna utveckling kommer att förändra mycket i grunden: vad vi gör, hur vi gör det och vad som går att göra. Informationen kommer att flöda i allt större mängder, genom och mellan organisationer och till och från privatpersoner. Exempelvis kommer kommunens information att tillgängliggöras i högre grad genom individuellt anpassade digitala tjänster och service, förvaltningar kommer att göras mer transparenta, och medborgare kommer i högre grad att kunna föra dialog med beslutsfattare.

Parallellt med digitaliseringens möjligheter finns också utmaningar och hot. Information är inte längre organisationsinterna tillgångar och angelägenheter, utan flödar mellan organisationer i

näringsliv och offentlig förvaltning, till och mellan enskilda, och över nationsgränser. Gränser suddas ut mellan vem som ”äger” och bär ansvar för viss information, vilket gör att det blir svårare att definiera hur den får användas och vem som kan och får ändra informationen, var ursprungsinformationen finns osv.

I och med att Internet är en arena för hela samhället är det också en plats för samhällets baksidor. Virus och annan skadlig kod, bedrägerier, utpressning, stölder, näthat och stalking (förföljelse) är företeelser som finns i olika former på nätet. Organiserad kriminalitet, extrema aktivistgrupper, terroristgrupper och stater har för längesedan flyttat delar av sina verksamheter på internet. Idag behöver man inte vara en IT-expert för att utföra destruktiva handlingar på nätet, utan tjänster kan köpas på välorganiserade marknadsplatser där handel sker anonymt och krypterat. Löpande sker mängder av informationsrelaterade incidenter i Sverige och internationellt som beror på avsiktliga attacker såväl som misstag och olyckor.

Dessa trender innebär sammantaget stora utmaningar för kommunens informationssäkerhet och dataskydd. Hedemora kommun ska arbeta aktivt för att skapa e-förvaltning med digitala tjänster och informationen är för Hedemora kommun en strategisk resurs som genomsyrar alla våra verksamheter.

Denna utveckling där informationshantering och informationsflöden antar nya former i samhället, i kombination med en ökad och förändrad hotbild, innebär att en god informationssäkerhet och ett gott dataskydd är en förutsättning för att Hedemora kommun kan delta i det digitala samhället.

Information och informationstillgångar

Information är en viktig resurs för Hedemora kommun och är av stor betydelse för alla våra verksamheter. Den finns i kommunens alla verksamheter och är en i dagens samhälle värdefull, viktig och kritisk tillgång. Information innebär upplysningar om faktiska och tänkta förhållanden. Information kan innehålla uppgifter om personer, men behöver inte göra detta. Information kan uttryckas i och representeras av mänskliga tankar och kunskaper, ord som skrivs på papper, tal som förmedlas muntligt eller via telefon eller data i form av tecken och signaler i olika digitala och analoga media. Information är således främst i form av texter, men även bilder, symboler, filmer och ljud utgör information. Information som tillgång (informationstillgångar) handlar alltså om mer än information som hanteras av IT-system.

Viss information är känslig/konfidentiell och måste skyddas från obehöriga att ta del av. Det kan handla om extra skyddsvärda och känsliga personuppgifter eller annan information som är sekretessbelagd med hjälp av offentlighets- och sekretesslagen (t ex information som är säkerhetsskyddsklassificerad eller information som är sekretessbelagd enligt speciallagstiftningar) och lagen om företagshemligheter. Det är också viktigt att information skyddas mot oönskad förändring och att den är åtkomlig och användbar av behörig vid rätt tillfälle, dvs att informationen hela tiden är riktig och tillgänglig. Det handlar ofta om hänsyn till den personliga integriteten, som är en mänsklig rättighet, och för att undvika att enskilda individer kommer till skada. Det kan även handla om skydd för andra mänskliga rättigheter, företagshemligheter, Sveriges säkerhet (försvaret inkl. civilförsvaret, det demokratiska statsskicket, rättsväsendet och nationell samhällsviktig verksamhet) och annan samhällsviktig verksamhet (t ex elproduktion).

Inventering av informationstillgångar och processer

(ISO 27002 8.1)

En grundläggande förutsättning vid hantering av informationstillgångar är att organisationen har inventerat vilka informationstillgångar som finns och har kontroll över dessa genom att veta var de finns och hur de hanteras och lagras under hela livscykeln etc. Livscykeln för information omfattar skapande, bearbetning, lagring, överföring, radering och förstörelse. Ett processbaserat arbetssätt underlättar och är ovärderligt vid informationsförvaltningen för återsökning, dokumentstyrning och dokumenterad och bevarad proveniens. Digitaliseringen gör informationen anonym och osynlig om den inte kopplas till de processer där den hanteras. En förutsättning för digitalisering är att informationen är sökbar med metadata som är konstant.

Genom att arbeta processbaserat kan enligt informationsägaren direktiv säkerställs det att informationen hanteras korrekt, uppdaterad, konsistent och överensstämma med övriga register, t ex registerförteckningen för personuppgifter (DSO-diariet i Ciceron).

Nyttan med att processbaserat arbetssätt är att verksamheterna får dokumenterade arbetsprocesser och en dokumenthantering som är organisationsoberoende. Detta bidrar till transparens och förtroende, ett evidensbaserat och strukturerat arbetssätt och informationstillgångars bestående värde. Den är även till god hjälp för kommunen i arbetet att uppfylla den grundläggande regeln i förvaltningslagen att kommunen ska ha en GOD OFFENTLIGHETSSTRUKTUR.

Introduktion till informationssäkerhet

Information behöver olika slags skydd beroende på hur skyddsvärd informationen är. Det kan handla om **tekniskt skydd** såsom brandvägg i ett IT-nätverk och kryptering, **administrativt** i form av regler (som denna riktlinje och andra styrdokument) och/eller att man **fysiskt** skyddar utrymmen med hjälp av dörrar, passersystem, lås, skåp m.m. Medarbetares kunskap och medvetenhet är en av grundstenarna i informationshanteringen, t ex att arbeta på rätt sätt med pappersdokument och IT-system och att vara försiktig med känslig/konfidentiell information. Säkerhet är inte bättre än den svagaste länken, och det är viktigt att alla typer av skydd fungerar på ett bra sätt tillsammans. En stor del av Hedemora kommuns informationssäkerhet beror därför på hur den enskilde medarbetaren hanterar informationen. Det handlar om att bygga ett högt säkerhetsmedvetande som är en del av organisationskulturen. **Alla måste ta sitt ansvar!**

Informationssäkerhet handlar således om att skapa och upprätthålla lämpligt skydd av information. Detta innefattar information i alla dess former; text, ljud, bilder, film osv, och oavsett hur informationen lagras, bearbetas och kommuniceras. Det kan vara med stöd av IT, papper eller direkt av oss människor i form av tal. Medan IT-säkerhet fokuserar på IT-baserad informationshantering handlar informationssäkerhet alltså om all information, oavsett form. Detta inkluderar förutom information i IT-system och andra IT-resurser även pappersbaserad information och information som finns i våra huvuden.

Information och de resurser som används för att hantera information benämns informationstillgångar. Informationssäkerhet utgörs av tre aspekter; att informationstillgångar ska vara konfidentiell, riktig och tillgänglig.

Olika typer av händelser (incidenter), som kan vara avsiktliga eller oavsiktliga, kan försämra konfidentialiteten, riktigheten och/eller tillgängligheten hos informationstillgångar. Informationen kan på ett oönskat sätt t ex stjälas, raderas, förändras eller göras otillgänglig.

En viss informationsmängd har krav på sig gällande de tre aspekterna som kan vara interna eller härledas från rättsliga krav eller förväntningar och behov från externa aktörer. Rättsliga krav i

form av lagar, förordningar, föreskrifter och avtal ställer krav på en verksamhets informationshantering som ofta inbegriper krav på informationens konfidentialitet, riktighet och tillgänglighet. Dessutom har ofta externa aktörer behov och förväntningar som påverkar organisationens informationssäkerhet.

Vad som är lämplig nivå av skydd för en viss informationsmängd beror på dessa krav, hotbild, och i vilka situationer informationen hanteras – hur den lagras, bearbetas, kommuniceras osv.

Introduktion till dataskydd

EU:s dataskyddsförordning (General Data Protection Regulation - GDPR), som trädde i kraft den 25:e maj 2018, gäller som lag i Sverige. Förordningen kompletteras sedan med en svensk dataskyddslag (lag (2018:218) med kompletterande bestämmelser till EU:s dataskyddsförordning och en svensk förordning (Förordning (2018:219) med kompletterande bestämmelser till EU:s dataskyddsförordning).

Syftet med GDPR är att stärka integritetsskyddet för enskilda personer, ge enskilda personer kontroll över sina personuppgifter, harmonisera lagstiftningen i Europa, anpassa lagstiftningen till den ökade digitaliseringen, minska byråkratiseringen och skapa förutsättningar för den inre digitala marknaden.

Ett gott dataskydd är en viktig förutsättning för digitaliseringen i samhället. Det handlar om att respektera den enskilde individens integritet och hens rättigheter när det gäller personuppgifter. På så sätt kan man skapa en nödvändig tilltro till den offentliga verksamheten och uppfylla invånarnas förväntningar inom detta område. En individs integritet är en mänsklig rättighet och framgår bl a av EU:s rättighetsstadga artikel 8 – Skydd av personuppgifter och artikel 7 (rätten till privatliv). Varje individ äger själv sina personuppgifter och Hedemora kommun lånar bara den enskilde individens personuppgifter när man behandlar dessa i sin hantering av information. Ett gott dataskyddsarbete är ett värdegrundsarbete som stämmer väl överens med Hedemora kommuns värdegrund KRAM (Kundfokus, Respekt, Ansvar och Mod). Att arbeta med dataskydd handlar om ett systematiskt förändringsarbete i hela organisationen. Det sker inte utan ett proaktivt arbete från nämnd/bolags och ledningens sida. Det handlar om att bygga en dataskyddskultur som är en del av organisationskulturen.

För att man överhuvudtaget ska få starta en personuppgiftsbehandling måste de grundläggande principerna i artikel 5 GDPR vara uppfyllda och det måste finnas en laglig grund enligt artikel 6 GDPR att stödja sig på. Dessutom ska den registrerade ha informerats om personuppgiftsbehandlingen och sina rättigheter enligt GDPR. En risk- och sårbarhetsanalys ska även ha genomförts som visar på om det föreligger behov av en konsekvensbedömning eller inte innan en personbehandling kan påbörjas.

Riktlinjens omfattning

Denna riktlinje innehåller information och regler gällande säkerhet vid all hantering av information och information och regler gällande dataskydd inom Hedemora kommun inkl. de helägda kommunala bolagen, nedan nämnd Hedemora kommun alternativt kommunen. Vid avvikelse för specifika kommunala bolag, nämns deras företagsnamn särskilt.

Riktlinjen redovisar regler avseende informationssäkerhet för förvaltning, kontinuitet och drift av kommunens informationsverksamhet och dataskydd, vilka krav som ställs på en medarbetare/användare och chef för att upprätthålla god säkerhet och dataskydd samt organisatorisk styrning av arbetet med informationssäkerhet, dataskydd och digitalisering.

Riktlinjen gäller för allt informationssäkerhetsarbete och dataskyddsarbete inom Hedemora kommun och är en del av Hedemora kommuns informationsverksamhet och hantering av informationstillgångar.

Alla kommunens nämnder och helägda kommunala bolag omfattas av styrdokumentet, vilket innebär att det inte finns utrymme att besluta om lokala regler som avviker från denna. Denna riktlinje gäller även för externa aktörer när dessa använder sig av kommunens och dess bolags informationstillgångar.

Alla styrdokument och mallar finns på Hedemora kommuns intranät under ”Informationssäkerhet och GDPR”. För Hedemora Energi AB med dotterbolag finns även styrdokument och mallar i IT-systemet Centuri.

Struktur och läsanvisningar

För att ge god läsbarhet är dokumentet uppdelat i fyra kapitel (A-D) som riktar sig till olika målgrupper:

Kapitel		Innehåll	Primär målgrupp	Sid
A	Informationssäkerhet och dataskydd för medarbetare och chefer	Riktlinje för hur information, dataskydd och IT ska hanteras i olika situationer	Alla medarbetare och chefer	16
B	Styrning av informationssäkerhetsarbete, dataskydd och digitaliseringsutveckling	Se Handlingsplan för informationssäkerhet, dataskydd och digitaliseringsutveckling – Styrning. Organisation, ansvar och roller och	Alla som arbetar med informationssäkerhet, dataskydd, IT och digitaliseringsutveckling	37
C	Informationssystem i verksamhetsnära förvaltning	Informationssäkerhet och dataskydd i objekt t ex IT-system, applikationer, plattformar o liknande	Informationsägare, systemförvaltare, projektledare, systemadministratörer, IT-enhet, Informationssäkerhets- och dataskyddsråd, Digitaliseringsutvecklingsgrupp, Digitaliseringsprojektgrupp, dataskyddsspecialister, DSO.	37
D1	Informationssäkerhet i IT-miljön	IT-säkerhet, hur information och IT ska hanteras inom IT-miljön	Chef och medarbetare på IT-enheten (inkl. driftansvariga)	40

Riktlinjen hänvisar till olika dokument som är nödvändiga när detta dokument ska tillämpas. För daterade hänvisningar gäller endast den utgåva som anges. För odaterade hänvisningar gäller senaste utgåvan av dokumentet (inkl. alla tillägg).

Denna riktlinje är baserad på den svenska och internationella standarden SS-ISO/IEC 27002.

Inom parentes i rubriken till varje avsnitt hänvisas till kapitel/rubrik i standarden SS-ISO/IEC 27002. OBS! Det kan dock inte garanteras att hänvisningarna är helt fullständiga. För detaljerade hänvisningar gäller endast den specifika rubriken. För hänvisningar med fler underrubriker än vad hänvisningen hänvisar till gäller hänvisningarna även underrubrikerna.

Dispenser

Ansökan om dispens från styrdokument vad gäller informationssäkerhet och dataskydd samt godkännande av specifika säkerhetslösningar (dvs tolka om de uppfyller styrdokumentet) ska ställas till Informationssäkerhets- och dataskyddsrådet. Sådana ärenden ska beredas innan de

ställs till informationssäkerhets- och dataskyddsrådet av kommunens informationssäkerhets- och dataskyddssamordnare för att underlätta beslut. Exempelvis kan en riskanalys ingå i beredningen av ärendet.

Dispens får aldrig vara permanent utan ska ha en giltighetstid på som längst två år. Om behov av undantag kvarstår ska ärendet beredas på nytt och nytt beslut fattas om eventuellt godkännande. Viktigt i detta arbete är även att uppföljningar och utvärderingar sker enligt plan.

Termer och definitioner

Term	Definition
Adekvat skyddsnivå	EU-kommissionen kan fatta beslut om att ett land (tredje land – utanför EU/EES) har en tillräckligt hög skyddsnivå och man får då föra över personuppgifter dit utan något särskilt tillstånd. Personuppgifter får föras över till tredje land om man vidtar lämpliga skyddsåtgärder – särskilda garantier.
Agilt arbetssätt	En iterativ (betyder förenklat att arbetet utförs i cykler) och lättrörlig ansats byggd på kontinuerligt lärande, som ger möjlighet för organisationer att snabbt anpassa sig till förändring.
Allmän handling	Varje handling som har kommit in till eller är upprättad hos en myndighet och som förvaras hos myndigheten. Handlingen kan vara i pappersform, innehållet i en e-post, ett ljud- och eller videoband, en cd eller en diskett osv. Offentlighetsprincipen innebär att vem som helst får begära ut en allmän handling. Om inte sekretess föreligger ska handlingen lämnas ut. Gäller även kommunala bolag.
Autentisering	Kontroll av uppgiven identitet. Verifiering av att en användare eller IT-resurs är den som den utger sig för att vara.
Behandling (personuppgift)	En åtgärd eller kombination/serie av åtgärder som vidtas i fråga om personuppgifter eller uppsättningar av personuppgifter, vare sig det sker på automatisk väg eller inte, till exempel insamling, registrering, organisering, strukturering, lagring, bearbetning eller ändring, återvinning, inhämtande, framtagning, läsning, användning, utlämning genom översändande, spridning eller tillhandahållande på annat sätt, justering eller sammanförande, samkörning, blockering, utplåning, begränsning, radering eller förstöring.
Behörighet	Tilldelade rättigheter att använda information eller en IT-resurs på ett specificerat sätt.
Data	Representant av fakta i form av t ex tecken eller signaler som är lämpad för överföring, tolkning, eller bearbetning av människor eller av automatiska hjälpmedel. Uppgifter eller information om något, oftast i samband med mätningar eller rapportering, exempelvis personuppgifter. Data är alltså inte synonymt med dator.
Dataskydd som standard (privacy by default)	Innebär att den personuppgiftsansvarige ska se till att personuppgifter i standardfallet inte behandlas i onödan. T ex att de förvalda inställningarna i en tjänst för sociala medier är satta så att inte mer information än nödvändigt samlas in, delas ut eller visas. Man ska utforma t ex IT-system, applikationer och plattformar så att inte fler personuppgifter än nödvändigt behandlas.
Dispens	En befrielse i ett enskilt fall från att följa villkor som framgår av lag, förordning, föreskrifter, avtal eller interna styrdokument.
Fysisk säkerhet	Fysisk säkerhet ska förebygga att obehöriga får tillträde till områden, byggnader och andra anläggningar eller objekt där de kan få tillgång till konfidentiell information och förebygga skadlig inverkan på sådana områden, byggnader, anläggningar eller objekt samt skydda personal mot utåtagerande personer.
Gemensam personuppgifts-ansvarig	Personuppgiftsansvarig som fastställer ändamål och medel/sätten för behandling av personuppgifter gemensamt med en eller flera andra personuppgiftsansvariga.
Harmlösa personuppgifter	Personuppgifter som varken är särskilt skyddsvärda- eller känsliga personuppgifter. Har en lägre skyddsnivå än särskilt skyddsvärda- och känsliga personuppgifter.
Inbyggt dataskydd (privacy by design)	Innebär att man tar hänsyn till integritetsskyddsreglerna redan när man utformar ex vis IT-system, applikationer och styrdokument. Det är ett sätt att se till att kraven i dataskyddsförordningen (GDPR) uppfylls och att den registrerades rättigheter skyddas. Ett begrepp som används för att se till att

	personuppgiftsansvariga använder sig av tillgängliga tekniska lösningar och organiserar sig med beaktande av GDPR. I praktiken innebär det ett krav på att hela tiden förbättra sig tekniskt och organisatoriskt. I arbetet ska beaktas den senaste utvecklingen, genomförandekostnader och behandlingens art, omfattning, sammanhang och ändamål samt riskerna för fysiska personers rättigheter och friheter.
Information	Information innebär upplysningar om faktiska och tänkta förhållanden. Information kan uttryckas i och representeras av mänskliga tankar och kunskaper, ord som skrivs på papper, tal som förmedlas muntligt eller via telefon eller data i form av tecken och signaler i olika digitala och analoga media. Innebörd i data, dvs data tolkad av människor.
Informationsklassning	Att genom konsekvensanalys identifiera skyddsbehovet för en viss informationsmängd.
Informationssystem	System som insamlar, bearbetar, lagrar eller distribuerar och presenterar information.
Informationssäkerhet	Konfidentialitet, riktighet och tillgänglighet hos information. Informationssäkerhet ska förebygga att information obehörigen röjs, ändras, görs otillgängliga eller förstörs samt förebygga skadlig inverkan i övrigt på uppgifter och informationssystem.
Informationstillgång	Information som är av värde för organisationen, och även de resurser som hanterar den, exempelvis människor, papper, mjukvara, hårdvara och immateriella tillgångar (t ex rykte). Information och de resurser som används för att hantera information
Integrationsskyddsmyndigheten (IMY)	Före detta Datainspektionen (DI). Datainspektionen ändrar namn till Integrationsskyddsmyndigheten den 1 januari 2021. IMY är Sveriges nationella tillsynsmyndighet för behandling av personuppgifter.
IT-resurs	IT-baserad komponent som hanterar information, t ex system, verktyg, tjänster och infrastruktur i form av mjuk- och/eller hårdvara.
IT-säkerhet	Säkerhet i IT-resurser för att uppnå och upprätthålla informationssäkerhet.
KLASSA 1	KLASSA 1 handlar om informationssäkerhetsklassning och är Sveriges Kommuner och Regioners (SKR:s) modell för informationsklassificering. Viss information är mer känslig än annan. Behovet av skydd skiljer sig därför mellan olika typer av information och i olika situationer. Skyddsbehovet beror på legala krav och vilka konsekvenser det skulle få för verksamheten eller för enskilda individer om informationen sprids till obehöriga.
Konfidentialitet	Att information inte tillgängliggörs eller avslöjas av obehörig. Skydd mot obehörig insyn (säkerställande av att information är tillgänglig endast för dem som har behörighet för åtkomst).
Konfidentiell information	Med konfidentiell information i detta dokument menas särskilt skyddsvärda- och känsliga personuppgifter, sekretesskyddad information inkl. säkerhetsklassificerad information.
Känsliga personuppgifter	Känsliga personuppgifter är uppgifter om ras och etniskt ursprung, politiska åsikter, religiös eller filosofisk övertygelse, medlemskap i en fackförening, hälsa, en persons sexualliv eller sexuella läggning, genetiska uppgifter och biometriska uppgifter som används för att entydigt identifiera en person. I dataskyddsförordningen kallas de här uppgifterna särskilda kategorier av personuppgifter. Behandling av dessa typer av uppgifter är i princip förbjuden. De undantag som finns måste tillämpas mycket strikt. Behandling av känsliga personuppgifter kräver en högre skyddsnivå.
Ledningssystem	Ett ledningssystem beskriver hur en organisation styr sin verksamhet och fastställer principer för ledning av verksamheten. Det fungerar som ett verktyg för högsta ledningen att säkerställa att verksamheten bedrivs enligt fastställda lagar, förordningar, föreskrifter, avtal och styrdokument och som ett stöd för medarbetarna i deras dagliga arbete.
Loggning	Loggning innebär att man skapar spårbarhet, dvs möjligheten att i efterhand kunna upptäcka och verifiera brister i främst konfidentialitet och riktighet.
Offentlighetsprincipen	Var och ens rätt till insyn och kontroll av myndigheter, bland annat rätten att ta del av offentliga handlingar.
Personalsäkerhet	Personalsäkerhet ska förebygga att personer som inte är pålitliga från säkerhetssynpunkt deltar i en verksamhet där de kan få tillgång till konfidentiell information eller i en verksamhet som av någon annan anledning är säkerhetskänslig samt säkerställa att de som deltar i kommunens

	verksamheter har tillräcklig kunskap om informationssäkerhet, dataskydd och annat säkerhetsskydd.
Personlig integritet	Det finns ingen allmänt vedertagen definition på begreppet personlig integritet. Integritet är en inre egenskap som är olika hos olika individer. ”Rätten att få vara i fred” är en vanlig tolkning. ”Rätten att få sin personliga egenart och inre sfär respekterad och inte utsättas för kränkande behandling” är en annan.
Personuppgift	All slags information som direkt eller indirekt kan knytas till en (fysisk) person som är i livet. Även bild- och ljuduppgift om en (fysisk) person räknas som personuppgift, även om inga namn nämns. Krypterad eller kodad uppgift är också en personuppgift om någon har en nyckel som kan koppla den till en person.
Personuppgiftsansvarig	Personuppgiftsansvarig är den organisation/juridiska person (t ex offentlig myndighet, aktiebolag, stiftelse, förening) som bestämmer för vilka ändamål personuppgifterna ska behandlas och medlen/sätter/hur behandlingen ska gå till. Även en fysisk person kan vara personuppgiftsansvarig, vilket t ex är fallet för enskilda firmor.
Personuppgiftsbiträde	Personuppgiftsbiträde är den som behandlar personuppgifter för en personuppgiftsansvarigs räkning. Ett personuppgiftsbiträde kan vara en fysisk eller juridisk person, offentlig myndighet, institution eller annat organ (t ex leverantör av datasystem, konsult eller kommunens IT-avdelning). Ett personuppgiftsbiträde finns alltid utanför den personuppgiftsansvariges organisation. Personuppgiftsbiträdet får bara behandla personuppgifterna enligt givna instruktioner från den personuppgiftsansvarige. Biträdet bestämmer således inte själv för vilka ändamål personuppgifterna ska behandlas. Även om en personuppgiftsansvarig väljer att anlita ett personuppgiftsbiträde är det alltid den personuppgiftsansvarige som har ansvaret gentemot de registrerade. Personuppgiftsansvarig är skyldig att ingå ett personuppgiftsbiträdesavtal (PuB-avtal) med personuppgiftsbiträdet.
Personuppgiftsincident	En säkerhetsincident som leder till risker för människors friheter och rättigheter genom t ex oavsiktlig eller olaglig förstöring, förlust eller ändring eller till obehörigt röjande av eller obehörig åtkomst till personuppgifter som överförts, lagrats eller på annat sätt behandlats.
Profilering	Varje form av automatisk behandling av personuppgifter som består i att dessa personuppgifter används för att bedöma vissa personliga egenskaper hos en fysisk person, i synnerhet för att analysera eller förutsäga denna fysiska persons arbetsprestationer, ekonomiska situation, hälsa, personliga preferenser, intressen, pålitlighet, beteende, vistelseort eller förflyttningar.
Register	En strukturerad samling av personuppgifter som är tillgänglig enligt särskilda kriterier, oavsett om samlingen är centraliserad, decentraliserad eller spridd på grundval av funktionella eller geografiska förhållanden.
Registrerade	Den som en personuppgift avser, det vill säga handlar om.
Riktighet	Att information är korrekt, aktuell och fullständig. Skydd om oönskad förändring (skydd av information och behandlingsmetoder så att de förblir korrekta och fullständiga).
Rättslig grund	Ett lagligt stöd i dataskyddsförordningen för att behandlingen av personuppgifter ska vara tillåten.
Sekretess	Information som inte ska lämnas ut och bli allmänt tillgänglig. Sekretessbelagd uppgift innebär tystnadsplikt för den som har eller har fått befattning med uppgiften. Stöd för sekretess finns i offentlighets- och sekretesslagen (t ex information som är säkerhetsskyddsklassificerad eller information som är sekretessbelagd enligt speciallagstiftningar) och lagen om företagshemligheter.
Spårbarhet	Entydig härledning av utförda aktiviteter till en identifierad användare eller IT-resurs.
Stark autentisering	Kontroll av uppgiven identitet på två olika sätt.
Särskilt (extra) skyddsvärda personuppgifter – integritetskänsliga personuppgifter	Extra skyddsvärda personuppgifter är inte känsliga personuppgifter, men har getts en särställning som innebär att de har samma högre skyddsnivå som dessa. Extra skyddsvärda personuppgifter är personnummer, samordningsnummer, värderingar/värderande uppgifter, omdömen. viss ekonomisk information och annan information som ligger nära privatlivet (som rör någons privata sfär). Exempel: löneuppgifter, uppgifter om lagöverträdelser, värderande uppgifter från t ex utvecklingssamtal, uppgifter

	om resultat från personlighetstester eller personlighetsprofiler, uppgifter om sociala förhållanden.
Tillgänglighet	Att information är åtkomlig och användbar av behörig. Åtkomst till behörig person vid rätt tillfälle (säkerställande av att behöriga användare vid behov har tillgång till den information som de behöver för att kunna utföra sina arbetsuppgifter).
Utgivningsbevis	En webbplats som har ett utgivningsbevis får grundlagsskydd enligt yttrandefrihetsgrundlagen och då gäller inte reglerna i dataskyddsförordningen i den mån det skulle inkräkta på den grundlagsskyddade rätten till yttrandefrihet.

Ledningssystem för informationssäkerhet, dataskydd och digitaliseringsutveckling (ISO 27002 5, 6, 18.1, 18.2)

Hedemora kommun med förvaltningar och bolag ska årligen se över, granska och vidta eventuella behov av förändringar av samtliga styrdokument inklusive nödvändiga processer och deras samverkan kring informationssäkerhet, dataskydd och digitaliseringsutveckling. Detta för att säkerställa att ledningssystemet för informationssäkerhet och skyddet för den personliga integriteten är aktuellt och principen om ständiga förbättringar efterlevs. Det ska också säkerställa ledningssystemets fortsatta lämplighet, riktighet och verkan. Granskning och behov av eventuella åtgärder kan även vara nödvändiga vid betydande förändringar i verksamheten.

KAPITEL A – Informationssäkerhet och dataskydd för medarbetare och chefer

Inledning

Detta kapitel vänder sig till dig som är medarbetare och/eller chef i Hedemora kommun. Kapitlet omfattar även extern medarbetare som har åtkomst till Hedemora kommuns information, exempelvis inhyrda konsulter.

Riktlinjen beskriver det ansvar du har som medarbetare och/eller chef vid hantering av information i Hedemora kommun och vilka regler som gäller för att upprätthålla god säkerhet. Lokalt på förvaltning/bolag kan det beslutas om kompletterande rutiner och vägledningar, men dessa får aldrig avvika från denna riktlinje utan särskilt tillstånd (dispens).

Informationssäkerhet för medarbetare och/eller följer i stort en struktur enligt SS-EN ISO/IEC 27000-serien.

Personalsäkerhet (ISO 27002 7)

Personal är en av organisationens absolut viktigaste tillgångar. Inom ramen för informationssäkerhet handlar personalsäkerhet i grunden om två saker:

- att skydda informationstillgångar från otillåten påverkan av personal på dess konfidentialitet, riktighet och tillgänglighet,
- att skapa kunskap och säkerhetsmedvetande om informationssäkerhet, dataskydd och offentlighetsprincip hos personal för att styra så att människan är ett skydd snarare än ett hotobjekt.

En viktig del i detta är styrning av behörigheter, såväl till information och IT-resurser som till fysiska lokaler och utrymmen.

Före anställning (ISO 27002 7.1)

Bakgrundskontroll (ISO 27002 7.1.1)

Bakgrundskontroll syftar till att skydda värden i organisationen, däribland informations-tillgångar. Den ska göras före anställning.

Bakgrundskontroll av sökande till tjänster i Hedemora kommun ska ske genom verifiering av sökandes meritförteckning (CV), t ex genom kontakt med referenser och bekräftelse av påstådda akademiska och yrkesmässiga kvalifikationer, och verifiering av körkort om den sökande innehar körkort.

För kritiska tjänster som personer i ledningsgrupper och styrelser, högre chefstjänster, säkerhetstjänster inkl. informations-, IT- och cybersäkerhet och de som har åtkomst till känslig- och samhällsviktig information krävs en förstärkt kontroll, juridisk historik (belastningsutdrag (BRU) och mer omfattande verifiering av CV och personbilden. Den sökande ska själv inkomma till arbetsgivaren med BRU i ett obrutet kuvert som ska öppnas tillsammans.

För befattningar som har betydelse för Sveriges säkerhet och som omfattas av säkerhetsskyddslagen (2018:585) ska det i anställningsförfarandet genomföras en säkerhetsprövning. Säkerhetsprövning kan även ske under anställningens gång.

Säkerhetsprövning syftar till att förebygga att personer som inte är pålitliga ut säkerhetssynpunkt får arbeta med kommunens IT-system och andra IT-resurser samt information. Säkerhetsprövning görs för att klargöra om en person kan antas vara lojal mot de intressen som ska skyddas och i övrigt pålitlig ur säkerhetssynpunkt. Viktiga aspekter att utreda är eventuella dubbla lojaliteter, intressekonflikter, bristande säkerhetsmedvetande och andra sårbarheter. Säkerhetsprövning består av grundutredning och i de flesta fall registerkontroll samt i vissa fall särskild personutredning. Det är med stöd av säkerhetsskyddslagen bara tillåtet att göra registerkontroll inom ramen för säkerhetsprövning för personal som ska arbeta i säkerhetskänsliga delar av verksamheten.

Registerkontrollen ska genomföras innan en person genom anställning eller på annat sätt deltar i verksamhet som har betydelse för Sveriges säkerhet. De befattningar som är aktuella framgår av Hedemora kommuns säkerhetsskyddsplan. Registerkontrollen administreras av kommunens säkerhetsskyddschef.

Alla bakgrundskontroller ska ta hänsyn till gällande lagstiftning rörande hantering av personuppgifter.

Utbildning (ISO 27002 7.2.2)

Utbildning syftar till att säkerställa att de som deltar i Hedemora kommuns verksamheter har tillräcklig kunskap om informationssäkerhet- och dataskydd samt offentlighetsprincipen och i vissa fall säkerhetsskydd som är relaterade till deras roller för att uppfylla det krav på behörighet och kompetens som deltagandet kräver.

Nyanställda ska genom information delges ansvar och skyldigheter kopplade till informationssäkerhet, dataskydd och offentlighetsprincip samt ta del av informationssäkerhet, dataskydd och offentlighetsprincip enligt denna riktlinje och andra styrdokument (t ex utbildningsplan) senast vid anställningstillfället. Delgivning och utbildning ska ges kopplat till ansvar som följer med rollen, t ex informationsägarskap, chef, handläggare, assistent, nämndsekreterare osv.

Anställningsvillkor och information (ISO 27002 7.1.2)

Ansvar och uppgifter kopplade till informationssäkerhet och dataskydd ska framgå och dokumenteras i ansvarsprofiler eller befattningsbeskrivningar. Alla medarbetare har ett visst ansvar för hantering av information och ska informeras om detta vid anställningstillfället.

Under anställning

Medarbetares ansvar för information, utrustning, programvaror samt disciplinåtgärder m.m. (ISO 27002 8.1.3, 13.2)

Se rubrikerna ovan **Information och informationstillgångar, Introduktion till informationssäkerhet och Introduktion till dataskydd.**

Alla medarbetare har skyldighet att rapportera alla informationssäkerhets- och dataskyddsincidenter enligt gällande rutiner. Medarbetare är också skyldig att rapportera brister som misstänks kunna medföra negativ påverkan på Hedemora kommuns information till närmaste chef och vid IT-system och andra IT-resurser även berörd systemförvaltare. Vid frågor kopplade till dataskydd ska också förvaltningens/bolagets dataskyddsspecialist informeras. Incidenterna och bristerna kan röra sig om till exempel:

- IT-angrepp/intrång

- Skadlig kod
- Oskyddad känslig/konfidentiell information (särskild skyddsvärda och känsliga personuppgifter samt sekretessbelagd information)
- Brister i efterlevnad av denna riktlinje eller andra styrdokument kring informationssäkerhet och dataskydd

Medarbetare som har upptäckt en incident eller en brist där brott misstänks föreligga, ska inte själv försöka bevisa sådana. Detta då det kan försvåra framtida utredningar.

Hedemora kommun ser positivt på att medarbetare påtalar behov av förbättringsåtgärder och/eller lämnar förslag på förbättringsåtgärder till systemförvaltare, dataskyddsspecialist, informationssäkerhets- och dataskyddssamordnare eller närmaste chef.

Hedemora kommun ställer krav på att alla medarbetare:

- följer denna riktlinje och andra fastställda styrdokument inom informationssäkerhet och dataskydd,
- har kunskap om vilket/vilka IT-system och andra IT-resurser och vilken information i övrigt man är behörig att använda och ta del av,
- har kunskap om vad information, informationssäkerhet, personuppgift, personuppgiftsbehandling och informationssäkerhets- och personuppgiftsincident innebär,
- vet var man ska vända sig när man behöver hjälp med frågor kring informationshantering,
- meddelar närmaste chef det egna behovet av utbildning och fortbildning ifråga om informationssäkerhet, dataskydd och offentlighetsprincipen.

Kommunen kan genomföra loggkontroller i IT-system och andra IT-resurser samt och applikationer i enlighet med gällande rutin.

Arbetsplatsens utrustning och programvaror (ISO 27002 8.1.3, 8.3.1, 8.3.3, 11, 12.2.1, 13.2)

För den utrustning som du som medarbetare förfogar över gäller att:

- all installation och konfiguration, eller fysiska ingrepp (”öppna burken”) av IT-utrustning endast får utföras av IT-avdelningen eller av IT-avdelningen anvisad/godkänd person,
- fel ska omgående anmälas till IT-avdelningen via Helpdesk (IT-support för Hedemora Energi AB med dotterbolag),
- endast kommunens utrustning får användas för arbete inom ramen för ditt arbete om ej annat har överenskommits med din chef och dispens har beviljats enligt ovan,
- bärbar dator ska förvaras inlåst på arbetsplatsen när du lämnar densamma vid arbetsdagens slut. Om du tar med dig datorn från arbetsplatsen, ska den förvaras på sådant sätt att du har kontroll över den,
- smartphones och surfplattor eller motsvarande ska förvaras på sådant sätt att obehöriga inte får tillgång till dem. Kodlås ska alltid vara aktivt.

För programvaror gäller följande.

- Programvaror ska godkännas och installeras av IT-avdelningen eller av IT-avdelningen anvisad/godkänd person.
- Det är inte tillåtet att kopiera eller använda kommunens program utanför dess verksamhet.

- Om du är i behov av ytterligare programvaror eller hårdvara ska du anmäla det till din närmaste chef som ska göra en beställning enligt fastställda rutiner (Helpdesk – IT-support för Hedemora Energi AB med dotterbolag).
- Medarbetare ansvarar själv för installation/nedladdning av applikationer (”appar”) till sina smartphones/surfplattor eller motsvarande och att dessa inte äventyrar säkerheten kring kommunens nätverk eller informationshantering.

Distansarbete (ISO 27002 6.2.2, 8.3.1, 8.3.3, 19.1.1, 11, 13.2)

Med distansarbete avses alla former av arbete utanför kontoret, inklusive icke-traditionella arbetsmiljöer benämnda ”distansarbete”, ”flexibel arbetsplats” och ”virtuella arbetsmiljöer”. Som medarbetare ska du vid distansarbete följa nedanstående regler.

- Denna riktlinje och andra styrdokument kring informationssäkerhet- och dataskyddsfrågor gäller även vid distansarbete.
- VPN-uppkoppling till kommunens IT-miljö ska alltid användas.
- Du har som medarbetare ansvar för att ingen obehörig får åtkomst till information som innehåller särskilt skyddsvärda och känsliga personuppgifter, sekretessbelagd information ink. säkerhetsskyddsklassificerad information och även ansvar för att erforderliga skyddsåtgärder vidtas. Exempel på obehöriga är familj, vänner, kollegor från andra offentliga och privata organisationer och medpassagerare.
- Du får inte använda privatägd utrustning i behandlingen av Hedemora kommuns information.
- Privata nätverk får endast användas om de är skyddade med lösenord.

GDPR-checklista för digitala möten och videokonferenser

Se Rutin för Digital kommunikation.

Internet, molntjänster och sociala medier (ISO 27002 8.1.3, 10.1.1, 13.2)

Användning av internet och sociala medier ska vara förenlig med kommunens verksamhet och värdegrund. Information på internet och sociala medier ska t ex vara öppen, saklig och etisk och i övrigt i enlighet med kommunens kommunikationsplan. Publicera inte något på internet som är oärligt, osant, vilseledande eller kränkande. Tänk på att det som publiceras är synligt och offentligt för allmänheten, sprids snabbt samt finns kvar under lång tid. Tänk därför igenom innehållet noga innan du publicerar.

Som medarbetare måste man skilja på professionell och privat roll. Internet är i arbetet på Hedemora kommun främst ett arbetsverktyg och ska inte störa ordinarie arbetsuppgifter eller innebära merkostnader för kommunen. Internet får nyttjas för privat bruk. Tänk på att när du surfar på Internet representerar du Hedemora kommun och lämnar spår efter dig, dvs det finns möjlighet att se vilka sidor som besökts, av vem och när. För material på internet som ska användas i tjänsten, får nedladdning och installation av upphovsrättsligt material (datorprogram, film, musik m.m.) inte ske utan stöd i lag, avtal eller med skriftligt tillstånd från rättighetsinnehavaren.

- Att använda kommunens internet för nedladdning av filer i olika format för privat bruk (spel, musik, filmer m.m.) är tillåtet om det inte påverkar kommunens IT-tjänster negativt (nedladdning av stora filer, strömma video/musik under arbetstid). Välj seriösa leverantörer vid nedladdning!
- Att titta eller lyssna å material av pornografisk eller rasistisk karaktär är förbjudet. Förbudet gäller också material som är diskriminerande enligt de sju

diskrimineringsgrunderna eller har anknytning till kriminell verksamhet. Undantag kan medges av din chef för specifika uppdrag. Detta ska ske skriftligen.

Endast säkra webbplatser får användas (t ex HTTPS).

Vid användning av kommunens utrustning (dator, surfplattor och smartphones eller motsvarande) utanför kommunens nätverk får inte fritt WiFi användas, såvida inte utrustningen är VPN-ansluten. Fritt WiFi bör alltid undvikas. Att **rekommendera istället är att surfa via mobiltelefonens datauppkoppling (internetdelning). VPN-uppkoppling ska ALLTID användas!**

När du är utanför EU/EES-anslutna länder bör du undvika att ta med kommunens utrustning. Att ta med kommunens utrustning innehållande särskilda skyddsvärda- och/eller känsliga personuppgifter, sekretessbelagt information eller säkerhetsskyddsklassificerad information är **ALLTID FÖRBJUDET!**

Ingen konfidentiell information (särskilt skyddsvärda- och känsliga personuppgifter, sekretesskyddad information inkl. säkerhetsklassificerad information) får lagras i molntjänster, varken inom EU/EES eller i tredje land!

Personuppgifter får inte lagras i **molntjänster** utanför EU/EES-anslutna länder utan att uppfylla undantagen i regelverket kring överföring av personuppgifter till tredje land i enlighet med dataskyddsförordningen. Adekvat skyddsnivå måste föreligga eller att man vidtagit andra lämpliga skyddsåtgärder (särskilda garantier). Se även rubriken Överföring av personuppgifter till tredje land.

Behörighet och behörighetsadministration (ISO 27002 9.1.1, 9.1.2, 9.2.1, 9.2.2, 9.2.3, 9.2.4, 9.2.5, 9.2.6, 9.3.1, 9.4)

För att du som medarbetare ska få tillgång till kommunens IT-miljö (AD-konto, e-postadress, IT-system och andra IT-resurser och nätverk) krävs att:

- Du är registrerad i kommunens eller de kommunala bolagens HR-system (kommunen - lönesystemet Personec). Då får du automatiskt access till AD-konto, e-postadress och nätverk.
- Din närmaste chef lämnar en beställning till berörd systemförvaltare för aktuellt IT-system och andra IT-resurser och godkänner den behörighet som är nödvändig i IT-resursen för att du ska kunna utföra dina arbetsuppgifter.

Som medarbetare ansvarar du för att följa de regler som kopplas till behörigheten. När behörigheter tilldelas, ändras eller fråntas bedöms dessa aktiviteter utifrån användarens tilltänkta roll i systemet och med utgångspunkt i **”minsta möjliga behörighet”**. Behörigheter kan styras tekniskt och/eller organisatoriskt (via styrdokument).

Där det är möjligt ska kontroller av behörigheter göras minst en gång i kvartalet för att säkerställa att obehöriga inte har kvar sina behörigheter.

Endast av informationsägare utsedd personal får ha tillgång till källkoder.

Lösenord (ISO 27002 9.3.1, 9.4.2, 9.4.3)

Lösenord är strängt personliga och får inte göras känt för andra personer, dvs lösenord får inte lämnas/lånas ut till andra personer eller delas mellan kollegor. Detta gäller även till IT-supporten. Lösenord får inte heller skrivas ner och ligga framme uppskriven på en lapp. Bäst är att förvara lösenordet i minnet. Lösenord ska hanteras som värdehandlingar. I de fall en dator

delas av flera, ska ändå personliga inloggningar göras. Detta är viktigt för spårbarheten, för att kunna veta vem som har gjort vad i systemen.

Om en obehörig kommer över ditt lösenord och får tillgång till ditt användar-ID, kan den personen utföra aktiviteter i ditt namn. Aktiviteter som du då kan bli ansvarig för. Du lämnar spår efter dig när du är inloggad och arbetar i IT-systemen och andra IT-resurser. De inloggningsfunktioner som finns i systemen används bland annat för att spåra obehörig åtkomst. Loggningar för att spåra obehörig åtkomst sparas i fem år för att kunna beivra eventuella dataintrång eller andra oegentligheter.

Om arbetar Hedemora kommuns IT-miljö och har du glömt bort ditt lösenord eller av annat skäl behöver byta ut detsamma, använder du i första hand e-tjänsten på www.hedemora.se under Medarbetare. Andra alternativ är att ta kontakt med din lättekniker på förvaltningen/bolaget eller kontaktar din närmaste chef som får anmäla behov av nytt lösenord vid Helpdesk.

Om arbetar Hedemora Energis IT-miljö och har du glömt bort ditt lösenord eller av annat skäl behöver byta ut detsamma, använder du i första hand så kontaktar du IT.

Ett lösenord ska vara ”starkt”, det vill säga svårt att gissa för någon annan. Det ska därför inte kunna förknippas med dig som person och dessutom ha en viss längd och komplexitet för att det ska vara svårt eller ta lång tid för en angripare att knäcka. Undvik därför ord (gäller även baklänges), namn, nummer, serier av nummer eller bokstäver eller något som någon annan kan koppla till dig som person.

Användar-ID och lösenord används för att skydda information och det är därför viktigt att följa nedanstående krav för skapande och hantering av lösenord.

- Tilldelade personliga inloggningsuppgifter, så som lösenord och PIN-kod, ändras vid första användningen.
- Elektroniska meddelande, till exempel, e-post, innehållande inloggningsuppgifter i klartext undviks.
- Identiteten på en användare säkerställs innan inloggningsuppgifter tilldelas, oavsett ok informationen är ny förnyad eller tillfällig.
- Tillfälliga inloggningsuppgifter är unika för en användare och går inte att gissa.
- Användaren bekräftar mottagandet av inloggningsuppgifter.
- Lösenord ska innehålla minst 8 tecken. Kravet kommer i närtid att ändras.
- Olika lösenord ska användas för olika IT-system eller andra IT-resurser och för olika tjänster på webben även om de är jobbrelaterade. Samma lösenord ska inte användas privat och i jobbet.
- Automatisk minnesfunktion för lösenordet ska inte användas. Om man loggar in på webbsidor ska man inte låta webbläsare spara lösenordet.
- Lösenord ska bytas regelbundet. En gång per år kommer automatiskt ett meddelande som tvingar fram ett byte av lösenord. Om man arbetar i IT-system eller andra IT-resurser där lösenordsbyte inte är tvingande, ska man ändå byta ut lösenordet några gånger om året. Lösenord ska bytas direkt om misstanke finns att det har röjts.

Stark autentisering tillika flerfaktorsautentisering eller multifaktorautentisering (ISO 27002 9.4.2, 9.4.4)

Vid åtkomst till informationstillgångar med höga krav på konfidentialitet och/eller riktighet ska stark autentisering användas. Det handlar om särskild skyddsvärda- och känsliga

personuppgifter, sekretessbelagd information (inkl. säkerhetskyddsklassificerad information). Här är skydd genom endast användarnamn + lösenord inte tillräckligt.

Som stark autentisering räknas identifiering av en person och verifiering av personens autenticitet genom en kombination av **minst två av följande tre faktorer**:

- ett lösenord eller någonting annat som man vet,
- ett smartkort eller någonting annat som man har,
- ett fingeravtryck eller någon annan egenskap som man är.

Exempel på stark autentisering är e-legitimationer (ex BankID), Siths-kort, VPN-inloggning.

Det krävs även stark autentisering vid extern åtkomst till kommunens IT-miljö eller vid åtkomst över internet, även om informationen man då får åtkomst till i sig inte är förknippad med några höga krav avseende konfidentialitet och riktighet.

Om informationen endast får lämnas ut till identifierade användare/personer ska mottagarens identitet säkerställas. Mottagarens identitet kan säkerställas genom e-legitimation, engångslösenord, aktiva behörighetskort eller motsvarande.

Lagring och säkerhetskopiering/backup (ISO 27002 8.2.3, 8.3.1, 10.1.1, 11, 12.3.1, 13.2)

Det är viktigt att information lagras på ett säkert sätt och säkerhetskopieras så att den kan återskapas i händelse av diskkrasch, oavsiktlig radering, skadlig kod m.m. Säkerhetskopiering, ofta kallad ”backup”, är en väsentlig och helt nödvändig typ av säkerhetsåtgärd för alla organisationer. Säkerhetskopior ska lagras geografiskt åtskilt från originalmaterial för att skydda från fysiska incidenter och katastrofer som t ex brand eller översvämning. Om information lagras lokalt, kopiera snarast till ordinarie lagringsplats (ex vis nätverk).

Den information som sparas på kommunens servrar säkerhetskopiera kontinuerligt av IT-avdelning. Vart backup förvaras ska framgå i systemdokumentationen.

Se - **Rutin för digital lagring**

- Information ska lagras på nätverket så att den säkerhetskopieras. Det kan vara i specifika verksamhetssystem eller gemensamma filarenor (i Hedemora kommuns IT-miljö G: och för Hedemora Energis IT-miljö (K:).
- Om information behöver lagras på lokal hårddisk, se till att regelbundet kopiera över informationen till nätverket.
- Om information har gått förlorad, exempelvis att man av misstag råkat radera ett dokument, ska IT-support kontaktas via Helpdesk och IT-suppport för Hedemora Energi. Förhoppningsvis kan de då återskapa den senaste säkerhetskopian.
- Konfidentiell information får endast lagras i därför avsedda och godkända system och lagringsytor som har begränsad åtkomst, både vad gäller användare och administratörer av systemet och lagringsytan.
- Lokal lagring av konfidentiell information, t ex på en persondator, får endast ske om lagringsenheten eller filerna är krypterade av Hedemora kommun godkänd metod för kryptering. Vad gäller säkerhetsskyddsklassificerad information ska den vara inlåst i säkerhetsskåp och hanteras enligt särskild instruktion.
- Fysiska dokument som innehåller konfidentiell information ska förvaras inlåsta i brandskyddat godkänt säkerhetsskåp eller godkänt närarkiv.

- Endast godkända molntjänster är tillåtna att användas. Kontrollera vilka molntjänster som är tillåtna inom din verksamhet.
- Konfidentiell information får inte lagras i molntjänster.
- All lagring av flyttbara lagringsmedia och/eller enheter för lagring av personuppgifter och konfidentiell information ska vara dokumenterad och registrerad hos varje förvaltning/bolag.

Lagring och kassering av information i pappersform (ISO 27002 8.3.1, 8.3.3)

Arbete med sekretessbelagd information i pappersform (t ex personakter) och säkerhetsskyddsklassificerad information får endast ske i kommunens lokaler. Undantag gäller för arbete vid förhandlingar (t ex förhandlingar i domstol) och möten med aktörer som ärendet berör.

Konfidentiell information i pappersform ska alltid förvaras/lagras inlåst i brandskyddat utrymme (t ex brandskyddat godkänt närarkiv eller brandsäkert godkänt säkerhetsskåp) när man inte arbetar aktivt med informationen.

Rutin för lagring av förvaltnings- och bolagsspecifik information i pappersform ska finnas på varje förvaltning/bolag. Lagring ska ske enligt arkivlag.

Rensning och gallring av information i pappersform ska ske enligt arkivlag, gällande dokumenthanteringsplan och gallringsbeslut. Förvaltnings- och bolagsspecifik rutin för hur rensning och gallring ska genomföras ska finnas för varje förvaltning/bolag.

Pappersdokument som innehåller konfidentiell information måste vid kassering strimlas eller kastas i godkända säkerhetskärl.

Mobila enheter (ISO 27002 6.2.1, 8.2.3, 8.3.1, 8.3.3, 10.1.1, 11, 13.2)

Mobila enheter som tillhandahålls av Hedemora kommun kan vara smart telefon, surfplatta, bärbar dator och bärbara minnesdelar (t ex USB-minne, CD/DVD-skiva, extern hårddisk eller liknande).

För hantering av mobila enheter gäller följande regler.

- Alla mobila enheter ska vara registrerade och märkta (genomförs av IT-avdelningen).
- Mobila enheter som tillhandahålls av Hedemora kommun är personliga redskap och får inte lånas ut eller överlåtas till annan. Den får således inte nyttjas av annan den person som genom sin anställning får nyttja den.
- Uppsatta säkerhetsinställningar i enheter får inte ändras av annan än IT-avdelningen eller person som IT-avdelningen godkänt.
- Installerad programvara får inte kopieras eller installeras på annan enhet.
- Mobila enheter ska låsas med kodlås, lösenord eller tvåfaktorsinloggning. Pinkoder, fingeravtryck eller annan autentisering måste användas till smarta telefoner och surfplattor eller motsvarande. Då pinkoder används ska ej enkla pinkoder som 0000, 1234 etc användas och inte samma pinkod som används i andra sammanhang, t ex pinkod till bankomatkort.
- Konfidentiell information måste vara krypterad på mobila enheter med av kommunen godkänd kryptering. Konfidentiell information får inte hanteras i smart telefon, surfplatta eller annan mobil enhet om inte särskild av kommunen godkänd säkerhetslösning används, t ex av kommunen godkänd kryptering.

- Konfidentiell information på USB-minnen ska undvikas. Om USB-minnen används, får endast av kommunen godkänd kryptering användas.
- Viktig information bör inte lagras enbart på en bärbar enhet. Den ska snarast kopieras över till kommunens nätverk så att informationen säkerhetskopieras.
- Endast godkända programvaror får installeras på enheten.
- Endast av kommunen godkänd enhet och programvara får anslutas till kommunens nät. (Det innebär exempelvis att externa USB-minnen inte får sättas in i en dator som ägs av Hedemora kommun)
- Privat utrustning kan anslutas till kommunens gästnät.
- Enheten får enbart anslutas till trådlösa nätverk som är kända och lösenordskyddade. Vad som gäller vid användning av fritt WiFi, framgår under rubriken Internet ovan.
- Vid distansarbete måste godkänd säker utrustning och anslutning användas.
- Anslutning med kommunens VPN-anslutning från en privat dator är ej tillåtet.
- Det finns ett stort utbud av applikationer (appar) att ladda ner till den smarta telefonen eller surfplattan. Många av dessa appar kan innehålla skadlig kod. I syfte att minska denna risk är det endast tillåtet att ladda ned appar som tillhandahålls av Hedemora kommun eller finns på App Store eller Google Play.

För fysisk hantering av mobila enheter gäller följande.

- Försiktighet ska iakttas vid arbete i publika miljöer, exempelvis kan skärmen skyddas med sekretesskydd och/eller skärmfilter.
- Arbete med konfidentiell information får inte ske i publika miljöer.
- Mobila enheter får inte lämnas utan uppsikt och ska förvaras i säkert och skyddat utrymme.
- Vid förlust av utrustning, se rubriken Förlust av utrustning enligt nedan.
- Utrustning ska i övrigt vårdas och hanteras på det sätt som föreskrivs, t ex skyddas mot värme och fukt. Vårda utrustningen genom att exempelvis använda skärmskydd och skal.

Hedemora kommun är som arbetsgivare ägare till mobila enheter som tillhandahålls medarbetare av kommunen i tjänsten och även till den information som finns i dessa. Man bör därför som medarbetare vara medveten om att arbetsgivaren har rätt att ta del av t ex sms, foton och kalenderanteckningar.

Skadlig kod (ISO 27002 8.2.3, 8.3.1, 12.2, 13.2)

Skadlig kod är ett samlingsbegrepp för oönskad programkod som skapats i syfte att störa, skada eller utnyttja datorer, datornätverk och däri ingående programvara och operativsystem. Skadlig kod kan vara virus, maskar, trojaner, rootkits, bakdörrar, spionprogram eller ransomware.

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, inklusive sådana som finns i sociala medier. IT-utrustning som drabbas av skadlig kod, även ett smittat USB-minne, kan om det kopplas upp i kommunens nätverk sprida sig vidare i nätverket och orsaka stor skada. Därför får inte några upphittade eller okända USB-minnen stoppas in i Hedemora kommuns IT-miljö.

Kommunens datorer är utrustade med skydd mot skadlig kod. Detta innebär inte fullständig säkerhet, utan du som 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 godkänd IT-utrustning till kommunens nätverk.

- Var misstänksam och undvik att klicka på konstiga länkar eller fylla i irrelevanta uppgifter.
- Öppna bifogade filer endast om de kommer från en känd avsändare och en bilaga som är förväntad.
- Var observant på om IT-utrustning beter sig långsamt eller konstigt. Vid misstanke om skadlig kod kontakta IT-avdelningen.

Om du misstänker att din dator innehåller virus eller har påverkats av annan skadlig kod eller annat onormalt ska du:

- OMEDELBART STÄNGA AV DATORN!
- OMEDELBART ANMÄLA FÖRHÅLLANDET TILL IT-avdelningen.

Om du misstänker att någon obehörig använt din användaridentitet och varit inne i IT-systemet eller annan IT-resurs ska du:

- omedelbart byta lösenord,
- notera när du senast var inne i IT-systemet eller annan IT-resurs (år, mån, dag och tid),
- notera när du upptäckte intrånget (år, mån, dag och tid),
- omedelbart anmäla dina misstankar till din närmaste chef, systemförvaltare och vid personuppgifter – dataskyddsspecialist.
- dokumentera alla iakttagelser i samband med upptäckten och försök att fastställa om kvaliteten på din information har påverkats.

E-post (ISO 27002 8.3.1, 8.3.3, 10.1.1, 13.2)

Se - **Riktlinje för Digital kommunikation och Rutin för Digital kommunikation.**

Säkert beteende (ISO 27002 8.3.1, 8.3.2, 8.3.3, 11, 13.2, 13.2.1,16.1)

Som medarbetare ska du vara säkerhetsmedveten. Med det menas att du minst ska ha en generell kunskap inom informationssäkerhet- och dataskydd och kunskapen måste vara relaterad till förhållandena i din egen verksamhet och din egen arbetssituation. Säkerhetsmedvetande består både av kunskap och ett beteende som kunskapen uttrycks i. Du har en skyldighet att som medarbetare vara med att bidra till en informationssäkerhets- och dataskyddskultur på din arbetsplats. För att vara säkerhetsmedveten räcker det således inte att man bara följer reglerna utan det krävs också att du har en förståelse för informationssäkerhets- och dataskyddets betydelse för verksamheten i stort.

En stor del av kommunens information hanteras muntligt, i system och på papper. Vi kommunicerar dagligen informellt och formellt på detta sätt och vi måste bete oss särskilt försiktigt då vi hanterar konfidentiell information. Tänk på att det alltid finns informell information som inte i förhand är definierad och klassad, utan som skapas i det ögonblick det uttalas eller skrivs. Det kan vara t ex omdömen om chefer och medarbetare – skvaller, rykten m.m. – eller information som är en oförutsedd händelse, t ex ett brott. Sådan information kan vara känslig och är i så fall konfidentiell information.

Regelverk för säkert beteende i Hedemora kommun:

- Skriftligt material som innehåller konfidentiell information får inte ligga framme så att obehöriga kan läsa den.

- Vid arbetsdagens slut, när man lämnar arbetsplatsen för kortare stunder, när informationen inte används eller lokalen är obemannade ska skrivbordet vara tomt från konfidentiell (särskilt skyddsvärda- och känsliga personuppgifter, sekretessbelagd information inkl. säkerhetsskyddsklassificerad information) och kritisk verksamhetsinformation. Konfidentiell information och/eller kritisk verksamhetsinformation ska vara inlåst i brandsäkert godkänt säkerhetsskåp eller godkänt närarkiv. Skrivbordet ska även vara tomt från flyttbara lagringsmedia när man lämnar arbetsplatsen vid arbetsdagens slut. Om du tar med dig flyttbar lagringsmedia från arbetsplatsen, ska den förvaras på sådant sätt att du har kontroll över den.
- Konfidentiell information har en begränsad krets av behöriga. Det måste beaktas så att inte obehöriga kan höra sådan information på arbetsplatsen, både i arbetssituationer men även i informella sammanhang, t ex vid fikabordet. Man ska enbart tala i stängda utrymmen och även försäkra sig om att fysiska samtal eller telefonsamtal inte hörs i intilliggande rum.
- Endast öppen information får kommuniceras hörbart utanför arbetsplatsen, exempelvis vid fysiska samtal på tåget, eller i telefonsamtal i kassakön. Konfidentiell information får överhuvudtaget inte kommuniceras muntligt i publika lokaler.
- Konfidentiell information på datorskärmen ska vara skyddad från obehöriga. Skärmen ska låsas när man lämnar datorn, även för en kortare stund. Om man har ett sk smart kort till datorn ska detta tas ut då man lämnar arbetsplatsen.
- Personuppgifter ska destrueras eller avidentifieras så snart ursprungliga personuppgifter inte längre är nödvändiga för det eller de identifierade ändamålen och personuppgifterna kan och får rensas och/eller gallras utifrån arkivlag, gällande dokumenthanteringsplan eller gallringsbeslut.
- Du får inte släppa in obehöriga personer själva in i kommunens lokaler.
- Se till att dörrar och lås går igen och att ingen obehörig smiter in.
- Se till att fönster är stängda när du lämnar rummet/en lokal.
- Rapportera om du ser något misstänkt eller någon brist i skyddet (t ex misstänkt sabotage, trasiga dörrar, lås eller motsvarande).
- Var uppmärksam på besökare som verkar vilse och/eller utan passerkort eller besöksbricka.
- Att som besöksmottagare följa din besökare ut till ytterdörr alternativt reception/kundtjänst.
- Håll ordning på passerkort, kod och eventuella nycklar och låna aldrig ut dem till någon annan.
- Besökare får inte vistas utan uppsikt i lokaler där konfidentiell information kan finnas. Mottagare av besök ansvarar för besökare så länge de befinner sig i kommunens lokaler. Obekanta personer i sådana lokaler ska tillfrågas vem de söker och hjälpas tillrätta.
- Vid fysisk posttjänst ska konfidentiell information hanteras genom att förslutna brev ska användas för intern information som ska skickas internt i kommunen och rekommenderade försändelser ska användas om brev som ska skickas externt utanför kommunen. Se även gällande **Rutin för post- och diariehantering (Postrutin).** Konfidentiell information får inte fotograferas av med hjälp av digital kamera, smart telefon eller liknande.
- Kopiering av dokument som innehåller konfidentiell information ska begränsas till det minsta som behövs för att uppfylla det identifierade behandlingsändamålet. Vid säkerhetsskyddsklassificerad information gäller särskilt instruktion.
- Du får inte lämna meddelande som innehåller konfidentiell information på telefonsvarare.

- Då konfidentiell information överförs via fax ska man försäkra sig om rätt nummer (t ex använda sig av kortnummer) och att mottagarens fax är övervakad under överföringstillfället. Man ska inte lämna faxen innan överföringen är klar.
- Vid utskrift ska dokument omgående hämtas upp från skrivare. Vid utskrift av konfidentiell information ska utskriften övervakas så att man är säker på att ingen obehörig kan läsa informationen. Detta gäller även scanning.
- Det är förbjudet att i kommunens lokaler installera och använda tekniska produkter såsom smarta assistenter som ”Siri” och ”Alexa” eller andra liknande produkter som kan avlyssna vad som sägs innan kommunen genomfört en risk- och sårbarhetsanalys som dokumenterats. Dessa produkter kan finnas i t ex Smart TV, smarta telefoner osv.
- Smarta klockor får inte kopplas ihop med kommunens IT-resurser.
- Applikationer (appar) som samlar in bilder, ljud eller på annat sätt spelar in får ej installeras i jobbmobil eller surfplatta.
- Var vaksam och anmäl misstanke om incidenter, skadlig kod, intrång, brott osv!

Om du tillfälligt lämnar din arbetsplats under arbetsdagen (ISO 27002 8.3.1)

Vid tillfällen när du inte har uppsikt över din datautrustning ska du ALLTID tillfälligt låsa datorn med kortkommandot: CTRL+ALT+DEL, välj Lås datorn (eller Windowsknappen + L). Stäng alltid av datorn när du går hem för dagen.

Service på utrustning eller kassering/avveckling av utrustning/ lagringsmedier (ISO 27002 8.3.2)

Vid service på din utrustning (om den ska lämnas bort till annan än kommunens IT-avdelning) ska konfidentiell information tas bort. Utrustning inkl. lagringsmedier som USB-minnen osv som ska kasseras/avvecklas ska rensas från all information. Det måste vara säkerställt att tidigare lagrade personuppgifter inte kommer att vara tillgängliga. Detta kan ske bland annat genom att personuppgifter destrueras eller att man ger dem en form som inte tillåter identifiering eller återidentifiering av de registrerade (avidentifiering). Rådgör med din chef och systemförvaltare om du är osäker.

Förlust av utrustning (ISO 27002 8.3.1, 8.3.3)

Om du som medarbetare tappar bort eller på annat sätt förlorar kommunens utrustning (dator, smartphone eller surfplatta etc), ska händelsen omgående anmälas som incident enligt gällande rutiner för informationssäkerhets- och personuppgiftsincidenter. Vid stöld ska en polisanmälan göras. I vissa fall finns möjligheter att fjärradera information.

Om du som medarbetare tappar bort (inte har haft kontroll över utrustning) eller på annat sätt förlorat kontrollen på kommunens utrustning (dator, smartphone eller surfplatta etc) och får tillbaka utrustningen får utrustningen inte kopplas upp mot kommunens nätverk innan IT-avdelningen har kontrollerat utrustningen och installerat om utrustningens programvaror. Dylika händelser är att betrakta som en incidenter och ska anmälas enligt gällande Rutin för informationssäkerhets- och personuppgiftsincidenter

Personuppgifter

Se – ”**Riktlinje för GDPR-arbetet i Hedemora kommuns nämnder och bolag”** och andra styrdokument på kommunens intranät under rubriken Informationssäkerhet och GDPR.

Överföring av personuppgifter till tredje land

Överföring av personuppgifter till tredje land är när personuppgifter som behandlas i ett EU- eller EES-land blir tillgängliga för någon i ett land utanför EU/EES-området.

Exempel på överföring av personuppgifter till tredje land:

- När du skickar dokument som innehåller personuppgifter per e-post till någon i ett land utanför EU/EES.
- När du anlitar ett personuppgiftbiträde i ett land utanför EU/EES. Gäller även om personuppgiftsbiträdet anlitar underbiträden i tredje land.
- När du ger någon utanför EU/EES tillgång, exempelvis läsbehörighet, till personuppgifter som finns lagrade inom EU/EES.
- När du lagrar personuppgifter i en molntjänst som är baserad utanför EU/EES.
- När du lagrar personuppgifter, till exempel på en server, i ett land utanför EU/EES.
- När du har med dig mobiltelefon, dator eller surfplatta eller motsvarande vid resor utanför EU/EES-området och t ex e-post och kontakter finns förvarade i dessa.

För att det överhuvudtaget ska kunna vara tillåtet att föra över personuppgifter till tredje land krävs att det särskilda kravet på **adekvat skyddsnivå** uppnås i mottagarlandet eller att det finns lämpliga skyddsåtgärder (särskilda garantier) för att uppgifterna och de registrerades rättigheter skyddas. EU-kommissionen tillhandahåller uppgifter vilka länder det handlar om och uppgifterna uppdateras kontinuerligt. Uppgifter om vilka länder som är aktuella kan även finnas på datainspektionens webbplats. Se även rubriken Internet, molntjänster och sociala medier.

Det ska även framgå av registerförteckningen om personuppgifter i en specifik personuppgiftsbehandling får överföras till tredje land eller inte.

Medarbetare, chefer och uppdragstagare ansvarar för att nödvändiga skyddsåtgärder vidtas så att personuppgifter inte förs över till tredje land vid resor till eller mellanlandningar i dessa länder om tjänstemobil, tjänstedator, tjänstepadda eller motsvarande förs in i tredje land.

Informationssäkerhets- och personuppgiftsincidenter

Hantering av informationssäkerhetsincidenter och personuppgiftsincidenter samt rapportering av informationssäkerhetshändelser och personuppgiftsincidenter**,** se **– Rutiner för informationssäkerhetsincidenter och personuppgiftsincidenter m.m.**

Offentlighetsprincipen – Allmänna handlingar och sekretess

Offentlighetsprincipen är en grundläggande princip för Sveriges statsskick. I en av grundlagarna, tryckfrihetsförordningen (2 kap), finns det bestämmelser om bland annat rätten att ta del av allmänna handlingar. Denna rätt är ett uttryck för offentlighetsprincipen, som kallas för handlingsoffentligheten.

Det finns dock bestämmelser om sekretess som begränsar rätten att ta del av allmänna handlingar. Dessa bestämmelser hittar man i offentlighets- och sekretesslagen och lagen om företagshemligheter. Sekretess innebär begränsningar både i allmänhetens rätt att ta del av allmänna handlingar enligt tryckfrihetsförordningen och i offentliga funktionärers rätt till yttrandefrihet enligt grundlagen regeringsformen samt Europakonventionen, som gäller som lag. Sekretess innebär också begränsningar i den rätt att meddela och offentliggöra uppgifter som följer av tryckfrihetsförordningen och yttrandefrihetsgrundlagen.

Offentlighets- och sekretesslagen innehåller dessutom bestämmelser om bland annat myndigheters skyldighet att registrera allmänna handlingar, om överklagande av myndigheters beslut att inte lämna ut en allmän handling och om att kommunala företag och vissa enskilda organ ska tillämpa offentlighetsprincipen.

Informationshantering

Allmänna handlingar är de som finns förvarade hos myndigheten och antingen har inkommit till eller har upprättats i kommunen. De ska antingen registreras genom att diarieföras eller på annat sätt hållas ordnade. Allmänna handlingar ska hanteras i enlighet med gällande lagstiftning och kommunens styrdokument. Varje nämnd ska ha en Arkivbeskrivning där det framgår hur och i vilka system man håller olika typer av handlingar ordnade.

Allmänt kan sägas att det är bättre att diarieföra en handling än att låta bli, i synnerhet om det är tveksamt hur man ska göra. Detta för att underlätta att hålla ordning på handlingarna. Diarieföringen är en viktig hjälp för att kunna bevisa att handlingar har kommit in/skickats till myndigheten. Vissa handlingar måste enligt lag alltid diarieföras. Men det finns ändå en rad handlingar som man kan och ofta bör låta bli att diarieföra.

Vad ska diarieföras?

Sekretessbelagda allmänna handlingar måste i princip alltid diarieföras. Det åligger handläggaren att avgöra vad som ska diarieföras, men det är registratorerna som utför själva registreringen i diariet. Diarieföringen ska ske utan dröjsmål.

Huvudregeln är att in- och utgående skrivelser (även e-post, fax etc.) ska registreras som kommer från företag, annan myndighet eller allmänheten.

Exempel på handlingar som ska diarieföras:

- Avtal och kontrakt.
- Beslut eller interna skrivelser av formell karaktär.
- Beslut för överklagande på fråga om utlämnande av handling.
- Enkäter (där myndigheten ska svara, ej internt).
- Inkommande skrivelser som kan föranleda beslut, yttrande eller förslag.
- Inkommande skrivelser av väsentlig art för ärendet. Andra upplysningar kan skrivas in i ärendeanteckningar. Telefonanteckningar skrivs in i ärendeanteckningar.
- Hotbrev mot myndigheten eller enskild tjänsteman (ska omgående överlämnas till säkerhetschef).
- Utgående skrivelser (t.ex. remiss).
- Utlån av material.

Vad behöver inte diarieföras?

En allmän handling som uppenbart är av ringa betydelse för myndighetens verksamhet behöver inte diarieföras och gallras vid inaktualitet. Detta gäller t.ex. reklam, pressklipp, cirkulär och handlingar för kännedom som ej tillhör ett ärende, rutinmässig korrespondens.

Allmänna handlingar, för vilka sekretess inte gäller behöver inte registreras om handlingarna hålls ordnade så att allmänheten kan ta del av dem.

Exempel på handlingar som inte behöver diarieföras, men ska hållas ordnade:

- Enkla förfrågningar om information, fotokopior och liknande t.ex. förfrågningar om öppettider o. dyl.
- Fakturor.
- Förfrågningar om utlämnande av handling.
- Handlingar som inkommit för kännedom och som inte föranleder någon form av handläggning från myndighetens sida.
- Kallelse, dagordning, dokumentation till sammanträder, förhandling, kurs eller konferens.
- Kopior av andra myndigheters yttranden.
- Kopior rörande godshantering.
- Skrivelser för kännedom.
- Spam.
- Statistiska meddelanden.
- Trycksaker framställda av myndigheten (samlas i egen serie i arkivet).

Vad Ska inte diarieföras?
Allt som kommer till myndigheten är inte allmän handling och behöver därför inte diarieföras. Skada kan uppstå om denna typ av handlingar offentliggörs.

Exempel:

- Biblioteksförvarat material, handböcker eller liknande som förvaras i ordnade serier.
- Fackliga förtroendemäns handlingar.
- Politikers post som rör deras roll som partimedlem/partiarbete och inte som förtroendevald i kommunen.
- Felsända handlingar (om de är ställda till myndigheten ska de diarieföras).
- Författningstryck och offentliga utredningar som endast lämnas för kännedom.
- Minnesanteckningar (under förutsättning att de inte är justerade eller arkiverade).
- Privatbrev (brev som rör tjänstepersoners privatliv, blir inte allmän handling även om det skickats till myndigheten).
- Publiceringsmaterial (meddelande eller annan handling, som har inlämnats eller upprättats hos myndigheten endast för offentliggörande i tidskrift).
- Tidningar, tidskrifter och publikationer.
- Utkast till beslut eller skrivelse.

Medarbetaren är personligen ansvarig för säkerheten i sin hantering av information i alla dess former. Om medarbetaren uppmärksammar brister i kommunens informationshantering, ska detta omgående påtalas till närmaste chef.

Informationsklassning (KLASSA 1) ISO 27002 8.2.1, 11)

Viss information är mer känslig än annan. Behovet av skydd skiljer sig därför mellan olika typer av information och i olika situationer. Skyddsbehovet beror på legala krav och vilka konsekvenser det skulle få för verksamheten eller för enskilda individer om informationen sprids till obehöriga.

All information i Hedemora kommun ska genomgå informationsklassificering och sedan hanteras och lagras i enlighet med denna. Informationen i Hedemora kommun klassas utifrån Sveriges Kommuner och Regioners (SKR:s) modell för informationsklassificerings modell KLASSA 1, se även - KLASSA - Start (skl.se)**.** Informationsklassning i termer av rättsliga krav, värde, verksamhetsbetydelse och känslighet för obehörigt röjande eller modifiering. Informationsklassningen av informationen ska ske innan hanteringen startas och ska följas upp och genomgås minst vartannat år.

Den medarbetare som upprättar en handling eller tar emot en handling ska klassificera dokumentet och utifrån bedömningen säkerställa att informationen hanteras enligt gällande styrdokument. Samtliga IT-system och andra IT-system ska klassificeras.

Tas information ut ur något verksamhetssystem och lagras på annan media, eller används i ett annat sammanhang, måste informationen klassas om. Endast i undantagsfall får informationen lägre skyddsklass än tidigare. Samlas uttagen information med annan information finns det en stor risk att den aggregerade informationen får en högre skyddsklass än tidigare.

All information ska klassificeras utifrån konfidentialitet, riktighet och tillgänglighet och informationens värde.

Informationspyramiden nedan kan hjälpa till.

Informationspyramiden

All information ska var klassificeras vad avser Konfidentialitet/Riktighet/Tillgänglighet. Ju högre skyddsvärde/säkerhetsklass informationen har ju högre skydd på lagringsmediet och sätt att sprida informationen ställs det.

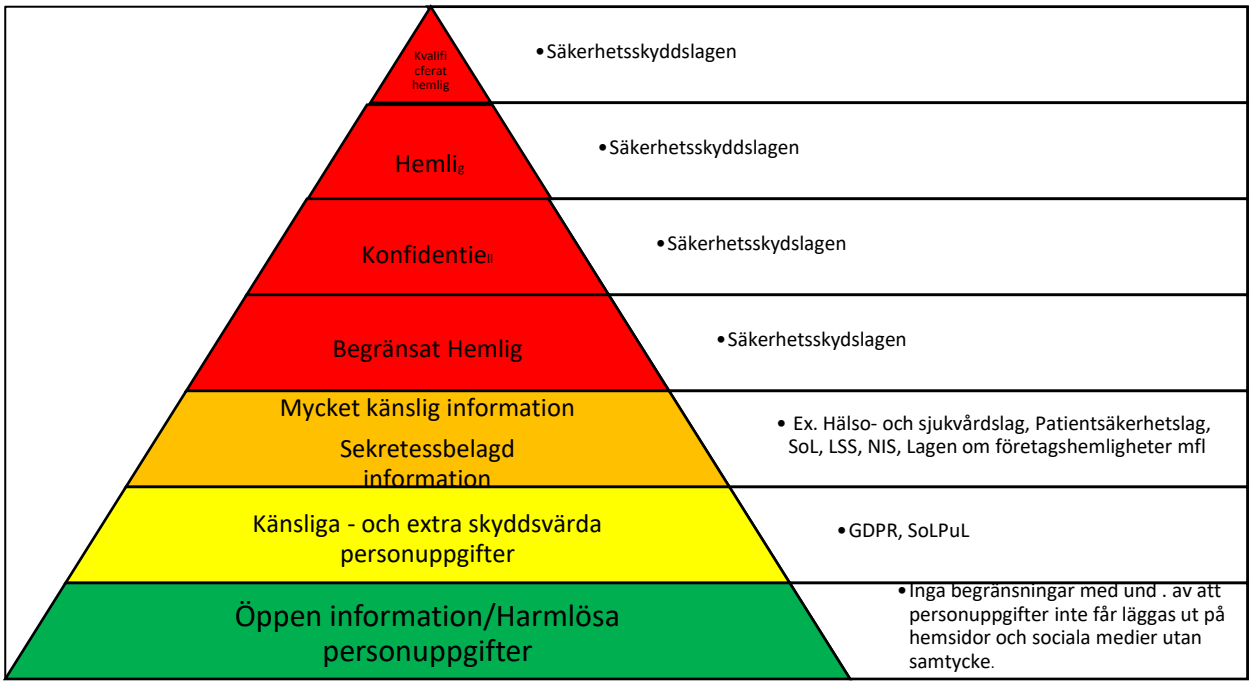


Bild 1: Informationspyramiden.

Öppen information - är information av allmän karaktär som får innehålla harmlösa personuppgifter. Information kan skickas med vanlig e-post och läggas ut på hemsidor. Offentliggörande av harmlösa personuppgifter på hemsidor och sociala medier (elektroniskt) kräver dock samtycke från den registrerade.

- **Lösenord och användar-ID räcker. Kräver inte någon kryptering.**
- **Information i pappersform kräver förvaring som är ordnad.**

Känslig information - innehåller särskilt skyddsvärda och känsliga personuppgifter i enlighet med GDPR.

- **Kräver tvåfaktorsinloggning och tydlig behörighetsstyrning. Kräver vid kryptering en end-to-end kryptering. E-post kräver säker e-post (TrustedDialog) med end-to-end kryptering.**
- **Information i pappersform kräver förvaring i godkänt brandskyddat låst säkerhetsskåp eller godkänt låst närarkiv.**

Sekretessbelagd information – Sekretessbelagd information enligt offentlighets- och sekretesslagen eller lagen om företagshemligheter

Är informationsmängd och innehållet tillräckligt omfattande kan dylik information beröras av **NIS-direktivet.**

- **Kräver tvåfaktorsinloggning och tydlig behörighetsstyrning. Kräver vid kryptering en end-to-end kryptering. E-post kräver säker e-post (TrustedDialog) med end-to-end kryptering.**
- **Information i pappersform kräver förvaring i godkänt brandskyddat låst säkerhetsskåp eller godkänt låst närarkiv.**

Begränsat hemligt och högre - Information som är klassad som hemlig enligt säkerhetsskyddslagen. Information upptill till och med Begränsad hemlig kan skickas med SIGNE. Konfidentiell och högre kan endast skickas med bud eller ordonnans.

- **Kräver tvåfaktorsinloggning och tydlig behörighetsstyrning.**
- **Information i pappersform kräver förvaring i godkänt brandskyddat låst säkerhetsskåp eller godkänt låst närarkiv.**

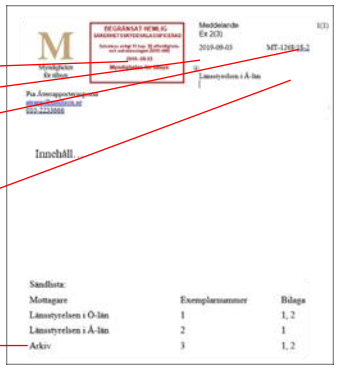
Observera att även samlad information, som är klassificerade i lägre nivåer än hemlig, tillsammans kan uppnå till någon av de hemliga nivåerna om de sparas samlat! Därför är det viktigt att ta höjd för eventuell aggregering tidigt vid hanteringen av information.

Märkning av information (ISO 27002 8.2.2, 8.2.3)

All information ska märkas (information i IT-system, applikationer och papper) med den klassificering informationen har fått vid klassificeringen vid tillämpande av KLASSA 1 (informationssäkerhet – konfidentialitet, riktighet och tillgänglighet), sekretessklassning (S), säkerhetsklassning (H) och GDPR-klassning (harmlösa personuppgifter, särskilt skyddsvärda personuppgifter, känsliga personuppgifter). Märkningen ska i IT-system framgå av systemet. Detsamma gäller applikationer.

Pappersdokument ska vid behov märkas på första sidan i det specifika dokumentet samt vid diarieföring anges i diariet med klassificeringsmärkningen.

- På första sidan ska det finnas:
  - Anteckning
  - Exemplarnummer
  - Sidnummer och antal sidor
    - Eventuella bilagor
    - Vilken handling bilagan tillhör
  - Beteckning (diarienummer)
  - Sändlista (Ex och mottagare)



Se - **Rutin för behandling av säkerhetsskyddsklassificerade uppgifter och handlingar m.m.**

Fysisk säkerhet (ISO 27002 11)

Fysisk säkerhet syftar till att:

- förebygga att obehöriga får tillträde till byggnader, områden, anläggningar eller andra objekt där de kan få tillgång till konfidentiell information,
- skydda dessa områden, byggnader och anläggningar från skadlig inverkan och
- skydda personal mot utåtagerande personer.

Fysisk informationssäkerhet handlar om utrustning (t ex persondatorer, servrar, mobiltelefon, surfplatta, skrivare, hårddisk och skärmar), lokaler, **utrymmen med särskilda skyddskrav (t ex IT-utrymmen – t ex datorhallar, serverrum och korskopplingsutrymmen, arkiv och kontorsutrymmen där känslig information hanteras) och elförsörjning.** Dessa lokaler ska ha godkänt brandskydd, ska bevakas och fysisk närvaro ska loggas (t ex tillträdesloggas). De ska ha ett skyddskrav på inbrottsskydd i skyddsklass 3 enligt norms SSF200 för inbrottsskydd.

Tillträde till utrymmen med särskilda skyddskrav ska hanteras restriktivt och endast ges till de personer som behöver tillträde för att utföra sitt uppdrag i den roll de har. Det ska finnas dokumenterade beslut om vem som ges tillträde att arbeta i utrymmena och det ska finnas rutiner som beskriver hur arbete får bedrivas i lokalen. Om arbete i utrymmen med särskilda skyddskrav utföres av obehörig personal/konsulter, ska ALLTID arbetet övervakas av behörig personal. Obehörig personal får ALDRIG lämnas ensamma i dessa utrymmen.

IT-utrymmen ska utformas så att utrustning inte utsätts för vätskeläckage, korrosiva brand-och släckgaser, damm etc.

Arkivlokaler ska bland annat ha skydd mot vatten och skadlig fukt, brand, brandgas och skadlig upphettning, skadlig klimat- och miljöpåverkan samt skadegörelse, tillgrepp och obehörig åtkomst.

Kritiska verksamheter som elförsörjning ska skyddas från avbrott och andra störningar. Fungerande reservkraftförsörjning som kan generera elektricitet oberoende av det allmänna elnätet måste finnas.

Exempel på säkerhetsåtgärder som på olika sätt kan användas för att skydda fysiska miljöer:

- Omslutningsyta, skalskydd, säkerhetszoner – lokals avgränsning mot andra lokaler och fria ytor, t ex väggar, golv, tak, dörrar och fönster.
- Brandskydd
- Lås och passersystem
- Smarta kort
- Kamerabevakning
- Besökshantering
- Larm
- Väktare

Spårbarhet och loggning (ISO 27002 9.4.2, 9.4.4, 12.4)

Loggning sker i kommunens 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.

Loggning gör det möjligt att i efterhand analysera händelser i IT-resurser och på så sätt

möjliggöra korrigerande eller förebyggande säkerhetsåtgärder. Loggning innebär att man skapar spårbarhet, dvs möjligheten att i efterhand kunna upptäcka och verifiera brister i främst konfidentialitet och riktighet. Exempelvis kan man upptäcka om medarbetare har överträtt sina åtkomsträttigheter och läst eller ändrat information som de inte haft rättighet till.

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

Det är helt avgörande att ”Rätt tid” fungerar vid loggningar. Rätt tid vid elektronisk kommunikation är något av det viktigaste vårt samhälle har. Klockor som går fel kan försvåra brottsutredningar och brottslingar kan gå fria. Systemklockorna i alla IT-system och andra IT-resurser ska synkroniseras mot en och samma referenskälla för tid.

Hedemora kommun bedriver loggning för att registrera följande aktiviteter och händelser:

- behandlingshistoriken av personuppgifter med angivande av läsning, ändring, utplåning eller kopiering av personuppgifter,
- användaraktiviteter, t ex inloggning och utloggning, lyckade och misslyckade åtkomstförsök till IT-resurser och transaktioner i IT-system och andra IT-resurser, applikationer och passersystem,
- systemavvikelser,
- förändringar i systemfiguration,
- användning av privilegierad åtkomst (administratörskonton)
- användning av systemverktyg och tillämpningar,
- alarm från system för åtkomstkontroll,
- aktivering, inaktivering och larm från säkerhetsverktyg, som anti-virussystem och intrångsdetekteringssystem.

Krav på säkerhets- och transaktionsloggar kan variera beroende på IT-resursens art och användningsområde. Det är verksamheters krav på IT-resursen och eventuella rättsliga krav som utgör grunden för behovet. Informationsägarna beslutar om vilka krav som gäller.

Loggkontroll genomförs enligt särskild rutin för loggkontroll för varje förvaltning/bolag.

Hedemora kommun har som arbetsgivare rätt att, utan att meddela medarbetaren, gå igenom dessa loggar för att kontrollera efterlevnad av lagstiftning och styrdokument. Vid misstanke om brott kan loggfilerna komma att lämnas ut till rättskipande myndighet utan att du som kontoinnehavare meddelas.

Disciplinåtgärder (ISO 27002 7.2.3)

Vid underlåtenhet att följa denna riktlinje och andra styrdokument kring informationssäkerhet och dataskydd samt offentlighetsprincipen följer Hedemora kommuns regler enligt lagar och avtal samt kommunens disciplinära process vid disciplinåtgärder. Misstänkt lagbrott enligt brottsbalken polisanmäls.

Ledningens/chefers ansvar för information och disciplinåtgärder (ISO 27002 7.2.1, 9.1.1, 9.2.1, 9.2.3, 9.2.4, 9.2.5, 9.2.6)

Chefer på alla nivåer har ansvar att kommunicera denna riktlinje och andra styrdokument kring informationssäkerhet- och dataskydd samt offentlighetsprincipen till medarbetare och relevanta externa parter och tillse att dessa får aktuell och relevant information, utbildning och fortbildning i informationssäkerhets- och dataskyddsfrågor samt i offentlighetsprincipen så att de kan utföra sina arbetsuppgifter i enlighet med gällande lagstiftningar, förordningar, föreskrifter och avtal.

Detsamma gäller att informera om regelverket kring tystnadsplikt och vid behov ingå avtal om sekretess. I ansvaret ingår att öka medvetenheten inom sin verksamhet om informationssäkerhet- och dataskyddsfrågor samt offentlighetsprincipen föra uppnå och vidmakthålla ett högt säkerhetsmedvetande och en god dataskyddskultur.

I ansvaret ingår att skapa medvetenhet och kunskap om incidentrapportering för att säkerställa att relevant personal är medveten om de möjliga konsekvenserna för nämnd/bolag (t ex rättsliga konsekvenser, förlust av affärer, varumärke eller skada på renommé) och även för personalen (t ex disciplinära konsekvenser) samt för den registrerade (t ex fysiska, materiella och känslomässiga konsekvenser) av att bryta mot informationssäkerhets- och dataskyddsreglerna.

Vid upphandling eller andra inköp ansvarar berörd chef för att krav ställs på leverantören att tillämpa informations- och dataskyddskraven i enlighet med Hedemora kommuns fastställda styrdokument, lagstiftning, förordningar, föreskrifter och avtal. Vid behov av avsteg gäller regelverket om dispens, se ovan. Leverantörers och verksamhetens ansvar för informationssäkerhet- och dataskydd samt sekretess ska framgå av avtalet med leverantören.

Vid underlåtenhet av medarbetare att följa denna riktlinje eller andra styrdokument kring informationssäkerhet- och dataskydd samt offentlighetsprincipen är berörd chef skyldig att vidta disciplinåtgärd i enlighet med Hedemora kommuns regler enligt lagar och avtal samt kommunens disciplinära process vid disciplinåtgärder. Misstänkt lagbrott enligt brottsbalken ska polisanmälas.

Närmaste chef för medarbetare som avslutar eller ändrar sin anställning har ansvar att säkerställa att åtkomsten till olika typer av IT-resurser (inkl. externa resurser som t ex molntjänster) och annan information som berör anställningen är strypt i direkt samband med avslut eller ändring av anställning. Det kan handla om användarkonton, åtkomsträttigheter och e-postkonton. Den ansvarar även för att säkerställa att IT-resurser mobiltelefon/smartphone, surfplatta, nycklar och passerkort eller liknande är återlämnade senast i direkt samband med avslut eller ändring av anställning. Om det finns risk att en medarbetare som slutar tar med sig känslig information, t ex till en konkurrent, kan man behöva logga och kontrollera medarbetarens aktiviteter.

Längre frånvaro – tjänstledighet, föräldraledighet och längre sjukfrånvaro

Vid längre frånvaro såsom tjänstledighet, föräldraledighet och längre sjukfrånvaro ska närmaste chef och medarbetare, om det går, kommunicera för att säkerställa tillgängligheten av information och IT-resurser som är knutna till medarbetaren. Chefen har ansvar för att initiera kommuniceringen.

Avslut anställning och ändring av anställning (ISO 27002 7.3, 8.1.4, 8.3.1, 9.1.1, 9.2.1, 9.2.4, 9.2.5, 9.2.6)

Vid avslut eller ändring av anställning kan ansvar och skyldigheter för informationssäkerhet- och dataskydd förbli gällande, t ex sekretessavtal och tystnadsplikt om medarbetaren haft tillgång till konfidentiell information. Lagstadgad tystnadsplikt gäller även efter anställningens avslut (t ex offentlighets- och sekretesslagen och lagen om företagshemligheter). Detta ska definieras och kommuniceras till medarbetaren vid anställning/tillträdande av roll och framgå i eventuellt sekretessavtal.

Som medarbetare ansvarar du för att det är ordning och reda på den information som du hanterat i din roll som medarbetare i Hedemora kommun. Det innebär bland annat att du ansvarar för att innan din anställning avslutas säkerställa att den information som ska vara diarieförd är

diarieförd och att övrig information har tagits om hand i enlighet med gällande dokumenthanteringsplan och/eller gallringsbeslut. Om du är tveksam eller har andra frågor, ansvarar du för att rådgöra med din närmaste chef. Notera att all information du framställt i din anställning vid Hedemora kommun är kommunens egendom.

Återlämnande av IT-resurser, mobiltelefon/smartphone, surfplatta, nycklar och passerkort eller liknande som kommunen äger/leasar och indrag av åtkomsträttigheter till information och IT-resurser (inkl. externa resurser som t ex molntjänster) ska ske i direkt samband med avslut eller ändring av anställning.

Chefens ansvar vid avslut, se under ”Ledningens/chefers ansvar för information och disciplinåtgärder” under rubriken Under anställning.

KAPITEL B – Styrning av arbete med informationssäkerhet, dataskydd och digitaliseringsutveckling

Ledarskap och engagemang, Policy, strategi, befattningar, ansvar och befogenheter inom organisationen (ISO 27002 5.1, 5.2, 5.3, 8.1.2)

Se - **”Informationssäkerhetspolicy och Dataskyddsstrategi”, ”Handlingsplan för informationssäkerhet, dataskydd och digitaliseringsutveckling – styrning” och ”Projektmodell för digitaliseringsprojekt i Hedemora kommun”.**

KAPITEL C – Informationssystem i verksamhetsnära förvaltning – styrning av driftsystem (ISO 27002 8.2.3, 9.4.4. 9.4.5, 10.1.2, 12, 12.5, 12.6, 14)

Införande och utveckling av informationssystem (IT-system och andra IT-resurser)

Vid införande och utveckling av informationssystem i form av IT-system och andra IT-resurser tillämpas adekvata delar av kommunens styrdokument ”Projektmodell för digitaliseringsprojekt i Hedemora kommun”. IT-system och andra IT-resurser och/eller komponenter som är relaterade till behandling av personuppgifter ska vara utformade enligt principerna för ”inbyggt dataskydd och dataskydd som standard”.

Driftgodkännande

Driftgodkännande avser den process som syftar till att fastställa om ett informationssystem uppfyller ställda säkerhets- och verksamhetskrav.

I samband med att en systemdokumentation upprättas, granskas om informationssystemet uppfyller de krav som ställs utifrån rättsliga, verksamhetsspecifika och hotrelaterade krav enligt förstudiens kravspecifikation.

Informationsägaren beslutar om driftgodkännande. Beslutet baseras på en granskning och säkerhetsutvärdering som bygger på jämförelse mellan verksamheternas krav och vidtagna säkerhetsåtgärder. Driftsgodkännandeprocessen relateras till aktuell kravspecifikation och ska omfatta:

- Avgränsningar.
- Granskningar av säkerhetsåtgärder i informationssystemet.
- Utvärdering av granskningen i förhållande till systemsäkerhetsplanens krav.
- Redovisning av beslutsunderlag.
- Beslut.

Beslutsunderlaget ska innehålla en sammanfattning av förslag till beslut som kan vara att:

- driftgodkänna informationssystemet/åtgärden,
- driftgodkänna informationssystemet efter beslut om när kompletterade säkerhetsåtgärder ska vara genomförda,
- inte driftgodkänna informationssystemet.

Avveckling av Informationssystem (ISO 27002 8.3.2, 9.4.4)

Informationssystem som inte längre behövs för verksamheten ska snarast avvecklas. Informationsägare ska efter samråd med systemförvaltare och driftansvarig besluta om och när ett informationssystem ska avvecklas.

Vid avveckling ska nedanstående särskilt uppmärksammas:

- Rättsliga regler såsom arkivlagen, dataskyddsförordningen, offentlighets- och sekretesslagen, dokumenthanteringsplan, gallringsbeslut m.fl.
- Vad som ska tas ut ur systemet före avveckling och i vilken form (papper eller datamedia).

- Om systemet innehåller ärenden som behöver avslutas i diarium eller dylikt, eller i annat system.
- Om återläsning av innehåll behöver kunna ske längre fram.
- Om uppgifter behöver flyttas över till annat informationssystem.
- Behandling av media som inte innehåller sekretessbelagd information.
- Destruktion av media och maskinvaror som innehåller sekretessbelagd information.

Drift

Kommunens regler för systemdrift är samlade i denna riktlinje under Kapitel D - **Informationssäkerhet i IT-miljön**. Kommunens tekniska IT-infrastruktur ska vara dokumenterad i särskilda systemsäkerhetsinstruktioner. Driftinstruktionerna ska årligen utvärderas och utifrån utvärdering ska erforderliga förbättringsåtgärder utföras.

Uppdateringar, underhåll och testning

I god tid innan arbeten påbörjas ska medarbetarna informeras om tid och eventuella begränsningar till informationssystemet.

Inför uppdateringar av systemet är rutinen att det ska finns en plan för hur och när uppdateringen ska genomföras. Planen ska innehålla datum för genomförande, hur medarbetarna ska informeras om att uppdateringen görs, vilka kontroller som ska göras för att kontrollera att uppdateringen fungerar och hur man ska agera om uppdateringen har misslyckats. Vid uppdateringar av viktiga och samhällsviktiga system bör tester genomföras innan arbetet startar.

Tester bör göras i miljöer som är åtskilda från produktionsmiljöer. Personuppgifter ska inte användas för testningsändamål. Fiktiva eller automatiskt genererade personuppgifter ska användas istället. Undantag kräver dispens, se ovan under rubriken Dispenser. Där användningen av personuppgifter för utvecklings- och testningsändamål inte kan undvikas ska tekniska och organisatoriska åtgärder som är likvärdiga med de som används i produktionsmiljön (skarp miljö) tillämpas för att minimera riskerna. Där sådana likvärdiga åtgärder inte är möjliga ska en riskbedömning göras och användas för att underbygga valet av lämpliga säkerhetsåtgärder. Planen ska godkännas av informationsägaren innan arbetet med uppdatering påbörjas.

Alla åtgärder ska dokumenteras.

Reservrutiner

Alla informationssystem bör ha reservrutiner. Samtliga samhällsviktiga informationssystem ska ha reservrutiner som är kända ute hos medarbetarna! Systemförvaltaren ansvarar för att ta fram reservrutiner, genomföra utbildningar med användarna samt att genomföra tillämpade övningar i störd IT-miljö. Övningar ska utvärderas och redovisas till informationssäkerhets- och dataskyddsrådet.

Vid störning där man har blivit tvungen att återläsa information måste verksamheten återskapa den information som man lagt i systemet efter det att senaste backupen gjordes. Rutin för att detta finns och övas ligger på systemförvaltaren att ta fram.

Systemdokumentation

Krav på och åtgärder för ett enskilt informationssystem ska dokumenteras i systemets system-dokumentation.

Uppföljning av loggar (ISO 27002 9.4)

Loggning syftar till att skydda informationen mot felaktig nyttjande.

Varje informationsägare måste utifrån gällande lagstiftning, förordningar, föreskrifter och avtal skapa rutiner för hur loggar ska hanteras, se även ovan under Kapital A rubrik Spårbarhet och loggning.

Incidenthantering

Att återkoppla erfarenheter från incidenter av olika slag är ett viktigt moment när det gäller att spåra brister och svagheter i informationssystemen. Beslutad Rutiner för informationssäkerhets- och personuppgiftsincidenter, som beskriver hanteringen av incidenter, ska följas.

Säkerhetschefen ska sammanställa och rapportera till koncernledningsgruppen alt kommunledningsgruppen i första hand och vid behov rapportera till utsedd statlig myndighet (MSB eller IMY).

Konsulters åtkomst till kommunens nätverk per extern anslutning

Det finns möjlighet för externa konsulter att få åtkomst till kommunens nätverk. Driftsansvarig meddelar tillstånd i varje enskilt fall. Konsulters tillgång till informationssystem ska avaktiveras direkt efter avslutat arbete. Konsulternas arbete i systemen ska dokumenteras i systemdokumentationen.

Personuppgiftsbiträdesavtal (PuB-avtal) ska finnas upprättat, i de fall, där personuppgifter behandlas och där PuB-avtal erfordras.

Kontinuitetsplanering (ISO 27002 17.1, 17.2)

Informationsägarnas krav på avbrotts- och katastrofplanering är samordnade i kommunens kontinuitetsplan. Se denna riktlinje under Kapitel D – Informationssäkerhet i IT-miljön.

D. Informationssäkerhet i IT-miljön

Inledning

Detta kapitel innehåller riktlinjer rörande säkerhet kopplade till IT-miljöer.

Riktlinjerna vänder sig därför främst till chefer och utsedda medarbetare. Riktlinjerna riktar sig också till externa parter som arbetar på uppdrag åt Hedemora kommun, exempelvis inhyrda konsulter.

Informationssäkerhet i IT-miljön kan även benämnas IT-säkerhet och innefattar säkerhet i olika slag av IT-resurser som system, verktyg och infrastruktur i form av hård- och mjukvara. Termen IT-resurser används genomgående i kapitlet på detta sätt som ett generellt samlingsnamn om ingen specifik hård- eller mjukvara avses.

Kapitlet är strukturerat utifrån nedanstående avsnitt i standarden SS-ISO/IEC 27002:2014 som till största delar innehåller säkerhet i IT-miljöer:

Rubrik	Kapitel i ISO 27002
Hantering av tillgångar	8
Styrning av åtkomst	9
Kryptering	10
Fysisk och miljörelaterad säkerhet	11
Driftsäkerhet	12
Kommunikationssäkerhet	13
Anskaffning och utveckling av IT-resurser	14
Incidenthantering	16
Kontinuitetshantering	17
Granskning och kontroll	18

Standarden innehåller mer vägledning och information än vad som finns i dessa riktlinjer, och standarden kan därför användas som ett stödjande dokument för att efterleva riktlinjerna.

Inom vissa områden i IT-miljön behöver mer detaljerade instruktioner tas fram som kompletterar eller konkretiserar dessa riktlinjer. Även för detta ändamål kan denna eller andra standarder liksom andra vägledningar, från t.ex. MSB, vara till stöd.

En central del i kommunens informationssäkerhetsarbete är informationsklassning. Information kan ha normala eller höga skyddskrav avseende konfidentialitet, riktighet och tillgänglighet i enlighet med Hedemora kommuns klassningsmodell (se Kapitel B). IT-resurser som hanterar information ska ges ett skydd i enlighet med dessa skyddskrav. Särskilda regler gäller i vissa fall för information som klassats enligt höga skyddskrav i en eller flera av aspekterna konfidentialitet, riktighet och tillgänglighet. Detta markeras genomgående med fetstil och rader i tabeller med riktlinjer har dubblerade linjer.

Roller och Ansvar

Ansvar för informationssäkerhet och IT-säkerhet följer ordinarie verksamhetsansvar. Det innebär att chefer och medarbetare inom respektive ansvarsområde ansvarar för att upprätthålla rätt nivå av informations- och IT-säkerhet för de processer och de IT-resurser de ansvarar för.

Se **Handlingsplan för informationssäkerhet, dataskydd och digitaliseringsutveckling – styrning** för mer information.

Hantering av tillgångar (ISO 27002 kap 8)

Alla system som finns ska återfinnas i respektives IT-miljös systemförteckningen.

Identifiering av IT-resurs och tilldelning av ägare (ISO 27002 8.1.2)

Samtliga IT-resurs ska vara identifierade och tilldelade en ägare och en förvaltare. Övergripande system som används av flera verksamheter ägas normalt av kommunstyrelseförvaltningen/IT-avdelningen. Vidare ska all IT-resurs ha en utsedd Driftansvarig samt en ersättare för denna.

Klassning av IT-resursen (ISO 27002 8.2.1)

IT-resurser ska klassas i enlighet med SKR:s modell för informationsklassning. Verksamhetssystem som klassats av den verksamhetsnära förvaltningen ska ges en nivå av IT-säkerhet som överensstämmer med verksamhetens krav så att rätt säkerhetsnivå upprätthålls. Underliggande IT-resurser i form av infrastruktur, stödsystem m.m. ska ges minst motsvarande klassning. Ibland kan sådana underliggande IT-resurser ges en högre klassning än de verksamhetssystem som de stödjer, exempelvis om IT-system stödjer ett flertal system som var för sig inte är kritiska.

Om det inte går att göra en koppling mellan IT-resurser och till klassade verksamhetssystem, får man klassa IT-resursen utifrån en bedömning enligt konsekvensbeskrivningarna i klassningsmodellen. Eftersom långt ifrån all information och alla system är klassade inom kommunen, kan preliminära klassningar behöva göras för IT-resurser. Vid osäkra fall är det viktigt att hellre ”överklassa” än att ”underklassa”.

Beroende på hur IT-resurser är klassade ska olika säkerhetsåtgärder införas för att uppnå ett tillräckligt bra skydd. Bland annat ska dessa riktlinjer följas som riktar sig mot IT-miljön och som i vissa fall har särskilda krav för IT-resurs som hanterar information med höga skyddskrav enligt en eller flera aspekter av konfidentialitet, riktighet och tillgänglighet. Ägare till IT-resurs ansvarar för att säkerhetsnivån är tillräcklig över IT-resursens hela livscykel, såväl vid införande, under drift som under avveckling.

Användningsinstruktioner (ISO 27002 8.2.3)

Det ska finnas regler och instruktioner till hur IT-resurs får användas. Dessa ska baseras på IT-resursens klassning och skyddskrav enligt ovan. Regler och instruktioner ska finnas oavsett om IT-resursen endast används inom digitaliseringsavdelningen, av medarbetare inom kommunen eller av externa användare. De som använder eller har tillgång till IT-resursen ska få instruktioner om hur de hanterar dessa resurser, vilka villkor och vilket ansvar som gäller kring den åtkomst de fått sig tilldelad.

Regler och instruktioner kan exempelvis avse användning av:

- Nätverk; t.ex. hur åtkomst till nätverk får ske, hur nätverkstjänster får användas, hur autentisering ska ske och hur utrustning som ansluts till nätverk ska identifieras
- Operativsystem; t.ex. hur åtkomst och autentisering ska ske
- Klientdatorer; t.ex. regler för programinstallationer som utförs av användare
- Annan lagringsmedia; t. ex. USB-minnen.

Krav

- ✓ Samtliga resurser ska identifieras och tilldelas en ägare, förvaltare och Driftansvarig.
- ✓ Samtliga resurser ska vara redovisade i Systemförteckningen.

- ✓ Resurser ska klassas baserat på klassningen av den information som hanteras i resurs och/eller baserat på klassningen av andra resurs som resursen stödjer eller påverkar.
- ✓ Skyddsåtgärder i en IT-resurs ska motsvara dess klassning så att rätt nivå av IT-säkerhet upprätthålls under resursens hela livscykel, såväl vid införande, under drift som efter avveckling.

Styrning av åtkomst (ISO 27002 kap 9)

Styrning av åtkomst är grundläggande för att skydda information och IT-resurser. Behörigheter innebär vissa rättigheter att använda en informationstillgång, exempelvis ett system, på ett specificerat sätt. Behörigheter, eller åtkomsträttigheter, definierar vad en användare har rätt att utföra, t.ex. läsa, söka, skriva, radera, skapa eller köra ett program.

Grundprincipen är att behörighetstilldelning ska baseras på användares behov till information eller till de IT-resurser (system, databaser, operativsystem eller nätverk) som dessa behöver för att kunna utföra sina arbetsuppgifter. Om information är strukturerad och klassad är det betydligt enklare att upprätta åtkomstregler och behörighetstilldelningar.

Inom vissa områden kan man behöva ha (teknisk) behörighet till en stor mängd information. Det kan vara svårt att på förhand definiera arbetsuppgifter, eller i akuta situationer måste kanske annan personal än den ordinarie snabbt ha åtkomst till information, som t.ex. inom vård och omsorg. Då får teknisk åtkomstkontroll ersättas av regelstyrd åtkomstkontroll, där regler säger att man inte får ta del av information som inte rör ens arbetsuppgifter. I sådana system är det särskilt viktigt med funktioner för uppföljning, övervakning och loggning.

Det samlade systemet för styrning av åtkomst i en (eller flera) IT-resurs(-er) benämns behörighetskontrollsystem (BKS) och utgörs vanligen av både tekniska system och administrativa rutiner. Ett BKS omfattar tre grundläggande säkerhetsåtgärder som tillsammans ska se till att verksamhetens säkerhetsregler (kontinuerligt) följs:

- Identifiering och autentisering av användares uppgivna identitet.
- Reglering av åtkomsträttigheter; vilken information man kommer åt och vad man kan göra med den, t.ex. läsa, skriva, ändra, radera.
- Loggning av användarens aktiviteter.

Identifiering och autentisering (ISO 27002 9.2)

Identifiering innebär att aktiviteter och åtkomst till en IT-resurs kan knytas till en individ, därför ska alla användar-ID vara unika och personliga.

Användar-ID och lösenord ger tillsammans en möjlighet till autentisering, dvs. verifiering av en uppgiven identitet. Vid åtkomst till information med höga skyddskrav avseende konfidentialitet och/eller riktighet ska stark autentisering användas. Som stark autentisering räknas identifiering av en person och verifiering av personens autenticitet genom en kombination av minst två av följande tre delar:

1. Ett lösenord eller någonting annat som man vet.
2. Ett smartkort eller någonting annat som man har.
3. Ett fingeravtryck eller någon annan egenskap som man är

Stark autentisering är också krav vid extern åtkomst till Hedemora kommuns IT-miljö.

Lösenord är alltid konfidentiella och ska i alla skeden av sin livscykel skyddas mot åtkomst från alla andra än ägaren själv. Det innebär att rutiner ska finnas som säkerställer att lösenordet

skyddas t.ex. från administratör eller handläggare oavsett om lösenordet tilldelas, förändras eller återställs.

Krav

- ✓ Alla användare ska ha en unik användaridentitet.
- ✓ Namn på användare, som underlag för t.ex. e-postadresser, ska vara enhetliga i kommunen och stämma överens med folkbokföringen.
- ✓ Vid åtkomst till information med höga skyddskrav avseende konfidentialitet eller riktighet ska stark autentisering användas.
- ✓ Stark autentisering är krav vid fjärråtkomst till Hedemora kommuns IT-miljö.
- ✓ Stark autentisering är krav vid fjärråtkomst till Hedemora Energis IT-miljö.
- ✓ Fjärråtkomst för inloggning med administrativa (priviligierade) konton till IT-resurs med höga skyddskrav avseende konfidentialitet eller riktighet är inte tillåten. Inlogg får endast ske via en Jump-host.
- ✓ Lösenord är alltid konfidentiell information som har höga skyddskrav och ska i alla skeden av sin livscykel skyddas mot åtkomst från alla andra än ägaren själv. För att minska risken för obehörig åtkomst ska följande skyddsfunktioner införas:
    - Tekniska funktioner implementeras där så är möjligt i IT-resursen för att säkerställa att lösenordsregler för medarbetare avseende historik, komplexitet och åldring av lösenord följs.
    - Lösenord ska aldrig skickas/transporteras i klartext över nätverk. I de fall detta inte är möjligt ska tillfälliga lösenord i kombination med tvingande lösenordsbyte användas. Tillfälliga lösenord ska enbart vara giltiga för en (1) inloggning.
    - Lösenord får aldrig lagras på ett sätt som gör det möjligt att dekryptera dem till klartext.
    - Om felaktigt lösenord används för inloggning i samhällsviktiga system mer än fem gånger ska aktuellt användar-ID utestängas och händelseloggen skicka ett meddelande till systemförvaltaren.
- ✓ För att minska risken för obehörig åtkomst ska samtliga klienter (datorer samt mobila enheter) förses med låsskärm så att skärm automatiskt låses efter en definierad tids inaktivitet och enbart kan aktiveras igen genom en förnyad autentisering.
    - Tidskrav 15 min för datorer
    - 60 sek för mobila enheter.
    - Alla medarbetare är ansvariga för att låsa skärmen när man lämnar datorn.

Reglering av åtkomsträttigheter (ISO 27002 9.4)

Åtkomst till resurs ska baseras på dess klassning, exempelvis ställs större krav på metoder för autentisering vid åtkomst till information med höga skyddskrav (se ovan).

För verksamhetssystem är det informationsägaren som beslutar vilka som ska få tillgång till systemet och vilka behörigheter dessa ska ha, samt hur systemet är klassat. Systemförvaltaren ansvarar för att upprätta ett BKS som motsvarar dessa krav.

Det ska finnas beslutade och dokumenterade regler och rutiner för behörighetshantering, dvs. BKS, i resursen. Detta inkluderar att underhålla och förvalta behörigheter, exempelvis hantering av beställning, ändring och borttagning av behörigheter och rättigheter. Förändringar i användares roller måste återspeglas i behörighetshanteringen, t.ex. att användare får andra arbetsuppgifter eller avslutar sin anställning.

Det ska finnas rutiner kopplade till personalavdelningen där man säkerställer att reglering av åtkomst sker vid anställning, vid förändring av roll eller arbetsuppgifter samt vid upphörande av anställning.

Innan någon tilldelas åtkomst till IT-resurs som innehåller uppgifter konfidentiell information, ska alltid prövning av den enskilde ske och en tystnads- och sekretessförbindelse upprättas och den enskilde ska utbildas i vad förbindelsen innebär och vilket ansvar som följer.

För externa användare gäller att tilldelning av åtkomst, utöver de regler som gäller all åtkomsttilldelning även ska vara tidsbegränsad för endast den tiden som behövs för att utföra uppgiften samt föregås av sekretessavtal.

För administrativa åtkomsträttigheter gäller att de ska vara restriktiva och ge endast de rättigheter som behövs för att utföra sitt uppdrag i den administrativa roll man har. Om funktion för privilegiehöjning finns ska sådan användas, t.ex. genom att använda ”sudo” i Linux/Unix eller att man efter inloggning utför vissa aktiviteter med ett konto med förhöjda rättigheter i Windows genom funktionen ”Kör som annan användare”. Vidare ska man där så är möjligt säkerställa att automatisk utloggning sker efter en definierad tids aktivitet vilken bör vara kortare än för normala användare.

Uppföljning och revision av samtliga åtkomsträttigheter ska ske en gång per år. För priviligierade användare med särskilda åtkomsträttigheter (administratörer) bör revision ske med kortare intervall. Särskild uppmärksamhet kan behöva ägnas då medarbetare med priviligierade åtkomsträttigheter slutar eller byter tjänst. Processer och rutiner för behörighetshantering ska följas upp och dokumenteras.

Krav

- ✓ Det ska finnas beslutade och dokumenterade regler och rutiner för behörighetshantering, dvs. BKS.
- ✓ IT-resurser ska ha åtkomsträttigheter som motsvarar hur de är klassade.
- ✓ Användaridentiteter och vilka individer dessa tillhör ska registreras i en gemensam förteckning och rutin ska finnas för att hålla denna förteckning uppdaterad. För att garantera spårbarhet ska rutinen även innehålla kontroll så att inte tidigare identiteter återanvänds. Historikfunktion ska finnas så att förteckningen kan visa vilka identiteter som fanns och vilka individer dessa tillhörde vid varje given tidpunkt.
- ✓ Åtkomst av Resurs ska vara registrerade i en förteckning med den åtkomst som beslutats och rutin ska finnas att hålla denna förteckning uppdaterad. Historikfunktion ska finnas så att förteckningen kan visa vilka identiteter och individer som hade åtkomst till en IT-resurs vid en given tidpunkt.
- ✓ Åtkomst som inte längre behövs eller behov av ny åtkomst ska regleras snarast, för IT-resurs inom en arbetsdag efter att behov upphör eller uppstår. Det ska finnas rutiner kopplade till personalavdelningen för att säkerställa att sådan reglering av åtkomst kan ske vid anställning, vid förändring av roll eller arbetsuppgifter samt vid upphörande av anställning.
- ✓ Administrativa rättigheter ska endast ges där så är uttryckligen nödvändigt och rättigheterna ska då vara tidsbegränsade. För tilldelning av administrativa rättigheter för användare på klienter gäller att sådan rätt i första hand ska ges tillfälligt för att t.ex. omfatta en installation av programvara och i andra hand ges för en viss tid med ett specifikt slutdatum. Informationsägare beslutar om tilldelning av priviligierad åtkomsträtt. Granskning av administrativa rättigheter ska ske en gång per månad.

- ✓ Gruppidentiteter är inte tillåtna. Eventuella undantag ska godkännas av **Informationsägare och säkerhetschef i förening.** Gruppidentiteter ska då enbart beviljas under följande förutsättningar:
    - Behov av gruppidentitet är tydligt beskrivet och alternativen utredda så att det framgår varför gruppidentiteten är nödvändig.
    - Gruppidentiteten ska ha en registrerad ägare.
    - Gruppidentiteten ska vara tidsbegränsade med tydligt slutdatum.
    - En avvecklingsplan ska finnas för att ersätta gruppidentiteten med individuella identiteter.
    - Ägaren av gruppidentiteten ska föra en förteckning alla som använder identiteten. Historikfunktion ska finnas så att förteckningen kan visa vilka användare som fanns vid en given tidpunkt.
    - Autentiseringsinformation ska uppdateras om någon användare lämnar gruppidentiteten.
    - Om en användare t.ex. lämnar en gruppidentitet med ett delat lösenord så ska lösenordet ändras och ett nytt lösenord distribueras till kvarvarande användare av gruppidentiteten.
    - Ägaren av gruppidentiteten tar fullt ansvar för eventuellt missbruk av gruppidentiteten.
- ✓ För externa användare gäller att tilldelning av åtkomst, utöver övriga regler för åtkomsttilldelning även ska:
    - Tidsbegränsas att endast omfatta tiden som behövs för att utföra uppgiften.
    - Föregås av sekretessavtal.
- ✓ Prövning av den enskilde ska ske och en tystnads- och sekretessförbindelse upprättas innan åtkomst tilldelas till IT-resurs som innehåller information med höga skyddskrav avseende konfidentialitet.

Loggning

För att erhålla spårbarhet och möjliggöra incidentutredningar och att i efterhand kunna utreda vad som hänt och för att upptäcka avvikelser från kommunens regelverk ska kommunens resurser övervakas och loggas avseende användaraktiviteter, avvikelser, fel och informationssäkerhetshändelser. Loggar ska skyddas mot manipulation och obehörig åtkomst, sparas en viss tid och granskas regelbundet av loggadministratör.

I de fall logginformation går att knyta till en enskild person är de att betrakta som personuppgifter och omfattas då av krav i personuppgiftslagen. Detta innebär bland annat att sådana loggar med personuppgifter ska skyddas från obehöriga. Det innebär också att om loggning används för att tekniskt övervaka ett system av säkerhetsskäl får loggen inte senare användas för andra syften. Om kontroller utförs för andra syften än det ursprungliga är lagkravet att personen ska informeras och ge sitt samtycke.

Krav

- ✓ Vid åtkomst till IT-resurs och information med höga skyddskrav avseende konfidentialitet eller riktighet krävs loggning av åtkomst för att erhålla spårbarhet.
- ✓ Loggningsverktyg och logginformation ska skyddas mot manipulation och obehörig åtkomst, logginformation innehållande loggning av åtkomst har alltid höga skyddskrav avseende konfidentialitet eller riktighet.

- ✓ Händelseloggar som registrerar användaraktiviteter, avvikelser, fel och informationssäkerhetshändelser, ska skapas, bevaras i fem (5 år) och granskas regelbundet.

För loggar som innehåller systemadministratörers aktiviteter gäller att de ska granskas av loggadministratör som inte är samma person som systemadministratören.

Kryptering (ISO 27002 kap 10)

Kryptering kan användas för flera ändamål, såsom att genom kryptering förhindra obehörig åtkomst till information, eller genom kryptografiska signaturer garantera informationens riktighet eller äkthet.

IT-avdelningen ska vid behov tillhandahålla godkända krypteringslösningar och instruktioner hur dessa ska användas. Behov av kryptering ska baseras på informationsklassning. Vanligen finns behov av kryptering då det föreligger **höga skyddskrav** på konfidentialitet och/eller riktighet.

Krypteringslösningar ska bygga på etablerade standarder och ska tas fram av IT-chef i samråd med verksamhetsansvarig och I informationssäkerhetssamordnare Införande av krypteringslösningar ska godkännas av informationssäkerhetssamordnare efter prövning av informationssäkerhetsrådet.

Ibland kan krypteringslösningar medföra nya risker relaterade till nyckelhantering. Dessa risker behöver hanteras bl.a. genom revokering, validering och återställning av nycklar:

- Revokering av nycklar gör det möjligt att avsluta åtkomst till IT-resurser.
- Validering av nycklars giltighet och autenticitet möjliggör att användare av en IT-resurs kan avgöra om en nyckel är giltig och att innehavaren kan kontrolleras.
- Återställning av nycklar är en funktion för att göra det möjligt att återställa information även om nyckel förloras. Detta kan t.ex. åstadkommas genom användandet av en särskild återställningsnyckel eller genom att nycklar säkerhetskopieras. Dock kan sådana lösningar innebära andra säkerhetsrisker eftersom nycklarna finns på fler ställen, och det ställer stora krav på åtkomstkontroll, administrativa rutiner och loggning så att åtkomst till nycklar kan spåras.

Krav

- ✓ Krypteringslösningar ska baseras på etablerade standarder och införande ska godkännas av informationssäkerhetssamordnaren efter prövning av informationssäkerhetsrådet.
- ✓ Nyckelhantering ska säkerställas för att tillgodose de krav som finns för resursen avseende:
    - Revokering av nycklar.
    - Validering av nycklars giltighet och autenticitet.
    - Återställning av nycklar.
    - Krypteringsnycklar är konfidentiell information och ska skyddas därefter.

Fysisk och miljörelaterad säkerhet (ISO 27002 kap 11)

Fysisk och miljörelaterad säkerhet avser att förhindra otillåten fysisk åtkomst till, skador på och störningar i resursen.

Generellt gäller att informationsklassning ska användas som ett stöd för att utforma det fysiska skyddet som alltid måste utgå från vilken information som hanteras samt hur skyddsvärd resursen är.

Säkra utrymmen (ISO 27002 11.1.1)

Säkra utrymmen med särskilda säkerhetskrav är exempelvis rum som används för servrar, switchar och annan kommunikationsutrustning, kontorsutrymmen där känslig information bearbetas samt arkiv. För IT-funktioner är det främst datorhallar, serverrum samt korskopplingsutrymmen som är aktuella.

Tillträden till säkra utrymmen ska vara restriktiva och endast ges till de personer som behöver tillträde för att utföra sitt uppdrag i den roll de har. Det ska finnas dokumenterade beslut om vem som ges tillträde att arbeta i säkra utrymmen. Det är verksamhetschefen som i samverkan med säkerhetschefen som fastställer vilka som ska ha tillträde till utrymmena.

Verksamhetsansvarig för ett säkert utrymme har också ansvar att ta fram en instruktion för hur arbete i respektive lokal får bedrivas. Personer med arbetsuppgifter i säkra utrymmen ska ha god kännedom om de regler som gäller för arbetet i dessa lokaler.

Säkra utrymmen ska utformas så att utrustning inte utsätts för vätskeläckage, korrosiva brand och släckgaser, damm etc. VA-dragningar i eller i direkt närhet av driftmiljö ska undvikas och risker för vatteninträngning hanteras. Om golvbrunn finns ska åtgärder vidtas för att undvika att vatten kan tränga upp.

Godkänt brandskydd och brandlarm ska finnas. Släckutrustning ska väljas så att inte onödig skada uppstår vid släckning av brand. Ventilation och andra genomföringar mellan brandceller ska förses med brandspjäll.

Säkra utrymmen som innehåller resurs med **höga skyddskrav** ska bevakas och fysisk närvaro ska loggas via passersystemet. Olovligt försök till tillträde ska skapa notifiering i passersystemets logg.

Godsmottagning och lastning [POSTHANTERINGSRUTIN] (ISO 27002 11.1.6)

Utrymme för godsmottagning och lastning ska avgränsas och organiseras så att de begränsar onödigt tillträde till känsliga områden och säkra utrymmen. Inkommande gods ska registreras och godkännas av egen personal vid leveranstillfället och eventuella avvikelser från förväntad leverans ska kvitteras av leverantören.

Underhåll, reparation och avveckling (ISO 27002 11.2.4, 8.3.2)

Underhåll av utrustning ska ske i enlighet med leverantörens anvisningar.

Reparation av utrustning och IT-resurser kräver ofta åtgärder från extern personal och auktoriserade reparatörer med utbildning på den utrustning som ska hanteras. Sådan personal har oftast varken behörighet till den information som hanteras i resursen eller tillträde till sådana säkra utrymmen där utrustningen finns placerade och detta kräver därför särskild uppmärksamhet.

Om underhåll och reparation ska utföras av utomstående på resurs med **höga skyddskrav** avseende konfidentialitet ska vederbörande alltid underteckna sekretessavtal. Det kan ibland vara nödvändigt att vidta särskilda åtgärder, t.ex. att känslig information flyttas, raderas eller krypteras innan någon utomstående hanterar utrustningen. Detsamma gäller avveckling av utrustning där avveckling eller återanvändning bör ske på ett sådant sätt att känslig information inte riskerar att komma i orätta händer. Datamedia där information inte har krypterats kan t.ex. behöva skrivas över eller destrueras på ett säkert sätt innan den sänds till skrotning eller återanvändning.

Skydd av utrustning (ISO 27002 11.1.1 - .5)

Utrustning ska placeras och skyddas för att skyddas mot stöld och miljörelaterade hot som värme, kyla, fuktighet, vätska samt partiklar i luft. Användning ska ske i enlighet med de instruktioner som framtagits av utrustningens ägare. Riskerna för åverkan och stöld är högre i vissa av kommunens egna lokaler, t.ex. där många externa personer frekvent vistas och i publika lokaler. Där krävs stöldskydd (t.ex. fastlåsning) och märkning.

Speciellt utsatt är också mobil utrustning där risken för förlust, stöld och skada är högre. Därför ska mobil utrustning som är avsedd att användas utanför kommunens lokaler förses med stöldskydd och märkning, undantaget mobiltelefoner. Användning ska ske i enlighet med de instruktioner som gäller vid distansarbete och mobil utrustning där användare t.ex. ska säkerställa att utrustning antingen övervakas eller låses in för att minska risken för stöld.

Elförsörjning (ISO 27002 11.2.2)

Säker elförsörjning (t.ex. avbrottsfri kraft genom UPS och reservkraft) ska finnas så att resursen skyddas från elavbrott och andra störningar som orsakas av fel i tekniska försörjningssystem.

Krav

- ✓ Tillträdet till säkra utrymmen ska vara begränsat och regleras minst med hjälp av låssystem med separat nyckelsystem. Nyckel-, kort- och kodinnehav ska vara förtecknade.
- ✓ Rutiner för att arbeta i säkra utrymmen ska utformas och tillämpas. Verksamhetsansvarig för ett säkert utrymme har också ansvar att ta fram en instruktion för hur arbete i respektive lokal får bedrivas.
- ✓ Beslut om vem som ges tillträde att arbeta i säkra utrymmen ska vara dokumenterat.
- ✓ Personal som beviljats tillfälligt tillträde till säkra utrymmen ska övervakas under hela besöket.
- ✓ Åtkomstpunkter såsom leverans- och lastningsområden och andra punkter där obehöriga personer kan komma in i lokalerna ska styras och om möjligt isoleras från säkra utrymmen för att undvika säkerhetsrisker och stölder.
- ✓ Inkommande gods ska registreras och godkännas av egen personal vid leveranstillfället och eventuella avvikelser från förväntad leverans ska kvitteras av leverantören.
- ✓ Godkänt brandskydd och brandlarm ska installeras. Släckutrustning ska väljas så att inte onödig skada uppstår vid släckning av brand. Ventilations och andra genomföringar mellan brandceller ska förses med brandspjäll.
- ✓ Utrymmet ska utformas så att utrustningen inte utsätts för vätskeläckage, korrosiva brand- och släckgaser, damm etc. VA-dragningar i eller i direkt närhet av driftmiljö ska undvikas och risker för vatteninträngning hanteras. Om golvbrunn finns ska åtgärder vidtas för att undvika att vatten kan tränga upp.
- ✓ Utrymmen som innehåller informationstillgångar med höga skyddskrav ska uppfylla Skyddsklass 3 enligt SSF 200 Inbrottsskydd.
- ✓ Serverrum ska skyddas från elavbrott och andra störningar som orsakas av fel i tekniska försörjningssystem.
- ✓ Kablage för ström och telekommunikation för data eller stödjande informationstjänster ska skyddas från avlyssning, störningar och skada.
- ✓ Åtgärder ska vidtas för att temperaturen hålls inom de gränsvärden som specificerats för aktuell utrustning, även vid störningar i elförsörjningen i de fall utrustning försetts med avbrottsfri kraft.

- ✓ Datamedia som innehåller för verksamheten kritisk information och systeminformation ska förvaras i för datamedia brandklassat datamedieskåp.
- ✓ Underhåll och reparation ska utföras på sådant sätt att information eller resurs inte riskerar att röjas eller skadas. Om utomstående ska utföra underhåll på resurs med höga skyddskrav ska sekretessavtal tecknas. Vid känslig information döljas, flyttas eller raderas från utrustningen. Underhåll och reparation ska följas upp i loggböcker.
- ✓ Avveckling eller skrotning av resurs och datamedia ska, efter att information som ska bevaras ha förts över Centralarkivet, ske genom att information skrivs över, raderas eller förstörs.
- ✓ Avveckling eller skrotning av datamedia med höga skyddskrav på konfidentialitet sker genom att information skrivs över i multipla operationer, alternativt att mediet där informationen lagrats förstörs på ett fullständigt och oåterkalleligt sätt. Observera att krypterad datamedia inte är känslig om nyckel för dekryptering ges ett fortsatt skydd, eller att nyckel destruerats.
- ✓ IT-utrustning ska inte avlägsnas utanför kommunens lokaler utan tillstånd.
- ✓ IT-utrustning tillhörande kommunen avsedd att användas utanför kommunens lokaler ska förses med stöldskydd och märkning.
- ✓ Konsulter som ska arbeta med resurs som hantera NIS-klassad information och uppåt ska vara säkerhetsskyddsklassad, så kallad SUA-upphandling ska vara genomförd.

Innan entreprenadarbeten utförs i säkra utrymmen ska en risk och sårbarhetsanalys genomföras. Alla åtgärder för att skydda utrustningen ska godkännas av Säkerhetschef och IT-chef.

Driftsäkerhet (ISO 27002 kap 12)

Driftsrutiner (ISO 27002 12.1)

Dokumenterade driftsrutiner ska finnas och göras tillgängliga för alla användare som behöver dem. Driftsrutiner ska finnas för väsentliga processer och resurs, såsom

- installation och konfiguration av system,
- uppstarts- och nedtagningsrutin,
- säkerhetskopiering (se nedan),
- underhåll av utrustning,
- supportkontakter vid oväntade funktionella eller tekniska problem,
- hantering av media och
- serverhall (se avsnitt D – Fysisk och miljörelaterad säkerhet).

Driftsrutiner ska vara formella och beslutade dokument.

Förändringar i resurs ska styras enligt fastställd rutin. Denna process ska säkerställa att alla ändringar som införs på tjänster, moduler och komponenter i IT-miljön är riskbedömda, planerade, kommunicerade, testade och godkända.

Utvecklings-, test- och driftmiljöer ska vara separerade för att minska risken för obehörig åtkomst eller ändringar i driftmiljön.

Om installationskontroller eller utbildning genomförs i resurs med **höga skyddskrav** kopplat till GDPR och/eller patentlagstiftning ska dessa dokumenteras för att kunna särskilja detta vid kontroll av loggar.

Krav

- ✓ Det ska finnas formella, beslutade och dokumenterade driftsrutiner för väsentliga processer och resurs. Dessa ska göras tillgängliga för alla användare som behöver dem.
- ✓ Ändringar i resurs ska följa fastställd process som säkerställer att ändringarna är riskbedömda, planerade, kommunicerade, testade och godkända.
- ✓ Utvecklings-, test- och driftmiljö.
- ✓ Tester i skarp miljö med höga skyddskrav ska dokumenteras.

Skydd mot skadlig kod (ISO 27002 12.2)

För att skydda mot skadlig kod behövs metoder för att förebygga, upptäcka skadlig kod och för att återställa IT-miljön efter angrepp. Förutom tekniskt skydd är det även viktigt att alla som använder IT-utrustning vet hur de kan minska risken att drabbas av skadlig kod samt vad de ska göra om de misstänker angrepp av skadlig kod (se Kapitel A, avsnitt A3 – Skadlig kod).

Kommunens resurs ska skyddas från skadlig kod genom att antivirusprogramvara installeras på klienter och servrar. Skyddet ska regelbundet uppdateras. Metoder att använda kan vara s.k. ”file reputation analysis” innan godtycklig kod tillåts exekveras eller ”web reputation analysis” för att system automatiskt ska kunna bedöma om webbsidor är säkra eller osäkra.

Programvara ska i förebyggande syfte skanna efter skadlig kod i

- datorer i kommunens nätverk,
- filer som tas emot via nätverk eller någon form av media och i
- webbsidor.

Resurs med höga skyddskrav ska regelbundet granskas med avseende på skadlig kod. Om angrepp av skadlig kod inträffat ska det finnas en fastställd rutin för återställning av resurs.

Säkerhetsuppdateringar är en viktig komponent för att hålla system och applikationer fria från säkerhetsbrister som kan exploateras av skadlig kod.

Det ska finnas rutiner för att regelbundet samla in information om skadlig kod, t.ex. prenumerera på nyhetstjänster eller bevaka webbplatser som ger information om ny skadlig kod (t.ex. cert.se).

Krav

- ✓ Det ska finnas metoder och programvara för skydd mot skadlig kod som förebygger, upptäcker skadlig kod och som återställer i kommunens IT-miljö efter angrepp.
- ✓ Alla datorer (servrar och klienter) ska ha skydd mot skadlig kod (antivirusprogramvara) som frekvent och regelbundet uppdateras (dagligen).
- ✓ Utrustning som stöder resurs med höga skyddskrav ska regelbundet granskas med avseende på skadlig kod.
- ✓ System och applikationer ska regelbundet uppdateras för att hållas fria från säkerhetsbrister som kan exploateras av skadlig kod. Säkerhetspatchar ska regelmässigt och skyndsamt installeras på alla resursens enligt tillverkarnas rekommendationer och enligt fastställd rutin.
- ✓ Det ska finnas en fastställd rutin för återställning av datorer om kommunen skulle drabbas av skadlig kod eller virusutbrott.
- ✓ Det ska finnas rutiner för att regelbundet samla in information om skadlig kod, t.ex. prenumerera på nyhetstjänster eller bevaka webbplatser som ger information om ny skadlig kod (t.ex. cert.se).

Säkerhetskopiering (Back-up) (ISO 27002 12.3)

Säkerhetskopiering av information, program och speglingar av system är en viktig del av driftsäkerheten. Detta ger möjlighet att återställa en resurs till ett fungerande tillstånd efter uppkomsten av ett fel, och att åtgärda både riktighet och tillgänglighet hos information.

Säkerhetskopieringen syftar till att väsentlig information ska kunna rekonstrueras med hjälp av säkerhetskopior och återlagringsrutiner. Dock är det inte alltid möjligt att återställa all information. Sådan information som tillförts systemet efter senaste säkerhetskopiering går normalt inte att återställa.

Det finns en viktig skillnad mellan säkerhetskopiering och spegling (redundans). Den sistnämnda ger enbart ett skydd för tillgänglighet och inte riktighet, eftersom informationen är identisk vid spegling vilket innebär att eventuell felaktig information då återfinns på båda ställen. Säkerhetskopiering och spegling är tillsammans nödvändiga skyddsåtgärder för resurs med krav på både riktighet och tillgänglighet.

Vilka skyddsåtgärder som vidtas för specifika system ska styras på av hur de är klassade i aspekterna tillgänglighet och riktighet. Stöd för detta kan vara att använda de två måtten RPO och RTO. Hur stor informationsförlust som kan accepteras kan definieras för varje IT-resurs genom att fastställa RPO (Recovery Point Objective). Den längsta acceptabla tiden för att återställa IT-resursen efter ett avbrott kan fastställas med målsättning för återställningstid RTO (Recovery Time Objective).

Säkerhetskopior ska lagras geografiskt åtskilt från originalmaterialet för att skydda från fysiska incidenter och katastrofer som t.ex. brand och översvämning. Ofta används lösningar där man skiljer på långtids- och korttidslagring där enbart långtidslagringen är skild från originalmaterialet. Då bör korttidslagring skyddas genom ett säkert utrymme avsett för datamedia, annars riskerar man att vid en brand förlora all information som tillförts systemet sedan kopiering till långtidslagring skedde, vilket i vissa fall kan vara lång tid (se avsnitt D4 – Fysisk och miljörelaterad säkerhet).

Säkerhetskopior ska testas regelbundet för att säkerställa att återlagring fungerar som avsett.

Krav

- ✓ För IT-resurser med höga skyddskrav avseende tillgänglighet ska redundans finnas i delkomponenter, system, lagring och nätverk samt säkerställd infrastruktur för IT-drift, t.ex. UPS elförsörjning, reservkraft, redundant kyla m.m.
- ✓ Tillgänglighet ska övervakas med automatiska larm om viktiga kvalitetsmått inte uppfylls. Gränsvärden för larm ska sättas så att uppfyllande av målsättning för återställningstid säkerställs. Automatiska larm ska regelbundet testas.
- ✓ Baserat på IT-resursens klassning av riktighet och tillgänglighet ska krav definieras för säkerhetskopiering av information. Dessa krav ska minst reglera vilken information som ska omfattas av säkerhetskopiering, hur lång tid som säkerhetskopior ska sparas samt vilka kontroller som ska genomföras av att säkerhetskopiorna fungerar.
- ✓ Vidare ska maximal informationsförlust och målsättning för återställningstid definieras för varje ITresurs och tillsammans med övriga krav ligga till grund för vald backuplösning.
    - Målsättning för återställning av data, RPO (Recovery Point Objective), den maximalt acceptabla mängden av dataförlust som tillåts vid en återställning av en IT-tjänst efter ett avbrott ska fastställas.

    - Målsättning för återställningstid, RTO (Recovery Time Objective), den längsta acceptabla tiden för att återställa resursen efter ett avbrott ska fastställas.
- ✓ Det ska finnas en process för återlagring från säkerhetskopia som är testad och dokumenterad för respektive resurs.
- ✓ Backup av resurs med **höga skyddskrav** avseende tillgänglighet (höga RTO krav) bör lagras på snabbt backupmedia såsom t.ex. SAN-diskar. Övervakning av backupfunktion ska konfigureras med automatlarm vid problem.
- ✓ Säkerhetskopiering av information med **höga skyddskrav** avseende konfidentialitet ska ske till krypterad backupmedia eller ges motsvarande skydd. Säkra återställningsrutiner ska användas med kontroller att återställning av konfidentiell information ges rätt skydd efter återställning, t.ex. bör dekryptering under återställning undvikas.
- ✓ Säkerhetskopior ska lagras geografiskt åtskilt från originalmaterialet. Om lösning används där man skiljer på långtids- och korttidslagring är det tillräckligt att långtidslagringen är skild från originalmaterialet under förutsättning att korttidlagrade säkerhetskopior förvaras i ett säkert utrymme avsett för datamedia.

Loggning och övervakning (ISO 27002 12.4)

Övervakning och loggning gör det möjligt att upptäcka händelser i resurs. Genom loggning kan man i efterhand analysera vad som hänt och på så sätt möjliggöra korrigerande eller förebyggande åtgärder. Händelseloggar som registrerar användaraktiviteter, avvikelser, fel och informationssäkerhetshändelser ska skapas, bevaras och granskas regelbundet.

Loggning av händelser utgör grunden för automatiserade övervakningssystem som är kapabla att skapa konsoliderade rapporter och varningar avseende säkerhet i system och tillämpningar.

Händelseloggar kan innehålla bl.a.

- användarkonto,
- systemaktiviteter,
- datum, tider och uppgifter om viktiga händelser, t.ex. inloggning och utloggning,
- enhetens identitet eller plats, om möjligt, och systemidentifierare,
- register över lyckade och misslyckade åtkomstförsök till system,
- poster av lyckade och misslyckade åtkomstförsök till data och andra resurser,
- förändringar i systemkonfiguration,
- användning av privilegierad åtkomst,
- användning av systemverktyg och tillämpningar,
- åtkomst till filer och typ av åtkomst,
- nätverksadresser och protokoll,
- alarm från systemet för åtkomstkontroll,
- aktivering och inaktivering av säkerhetsverktyg, som anti-virussystem och intrångsdetekteringssystem, och
- register över transaktioner som utförs av användare i tillämpningar.

Krav på loggar och övervakningssystem kan variera beroende på IT-resursens art och användningsområde. Det är IT-resursens klassning och resursägarens krav som utgör grunden för behovet.

Genom användning av loggverktyg samt att alla loggkällor använder gemensam och korrekt tid kan händelser i olika IT-resurser korreleras vilket ger en bättre och mera heltäckande bild av händelser jämfört med om logg övervakas i varje system för sig.

Loggar kan innehålla känsliga data och personinformation. Lämpliga säkerhetsåtgärder för ska därför vidtas.

Krav

- ✓ Loggning ska normalt ske i IT-resurser avseende fel, systemhändelser. Loggar ska sparas en viss tid samt regelbundet analyseras och övervakas. Typ och omfattning av loggar och övervakningssystem ska baseras på IT-resursers klassning och resursägares krav.
- ✓ För att säkerställa all typ av loggning av händelser ska systemklockorna i alla relevanta resurser synkroniseras mot en betrodd referenskälla för korrekt tid.
- ✓ Loggningsverktyg och logginformation har **höga skyddskrav** och ska skyddas mot manipulation och obehörig åtkomst.

Hantering av tekniska sårbarheter (ISO 27002 12.6)

Tekniska sårbarheter i IT-resurser kan innebära exponering för skadlig kod, dataintrång eller andra sårbarheter. Det ska finnas rutiner så att information om tekniska sårbarheter erhållas i tid, att sårbarheter kan analyseras och att lämpliga åtgärder kan vidtas för att behandla de risker som sårbarheter medför.

Krav

- ✓ Det ska finnas rutiner för att få information om, upptäcka, analysera och åtgärda tekniska sårbarheter i resurs. Uppdateringar och säkerhetspatchningar ska göras regelbundet på resurs.
- ✓ I de fall säkerhetspatchning inte är praktiskt möjlig, t.ex. för ”embedded” system eller SCADA-system ska information om tekniska sårbarheter i sådana resurs inhämtas och analyseras och lämpliga åtgärder vidtas för att hantera den tillhörande risken.
- ✓ Säkerhetsgranskning av resurs som exponeras mot Internet ska ske regelbundet och minst en gång per år för att kontrollera att inga uppenbara sårbarheter exponeras och att tillräcklig säkerhetsnivå upprätthålls. Sådan granskning kan t.ex. bestå av skanning av sårbarheter med automatiserade verktyg eller så kallade penetrationstester.
- ✓ Det ska finnas regler för programinstallationer som utförs av användare som definierar vilka typer av program en användare kan installera och på vilket sätt.

Kommunikationssäkerhet (ISO 27002 kap 13)

Kommunikationssäkerhet är skydd i resurs och nätverk som används för datakommunikation i syfte att skydda den information som kommuniceras.

Nätverkssäkerhet (ISO 27002 13.1)

Nätverk måste hanteras och styras för att skydda information i anslutna system och tillämpningar. Det ska finnas rutiner för hantering av nätverk och förvaltning ska ske av ansvariga som utpekas av ägare till nätverk.

Skyddsåtgärder ska införas för att nå säkerhet för information i nätverk och anslutna tjänster utifrån klassningen av anslutna resurs, dvs. krav på konfidentialitet, riktighet och tillgänglighet.

Krav på skydd ska inkluderas i avtal för nätverkstjänster om dessa tjänster tillhandahålls som outsourcade tjänster. Skydd för nätverkssäkerhet kan exempelvis vara:

- Autentisering av system
- Kryptering
- Regler för säkerhet och nätverksanslutning
- Begränsning av systemanslutningar
- Brandväggar och intrångsdetekteringssystem
- Loggning och övervakning av nätverk
- Separation av nätverk (segmentering)

Segmentering betyder att dela upp nätverket i olika segment för att t.ex. tillåta enbart ekonomiadministratörer tillgång till nätverket med ekonomisystem. Segmentering av nätverk ska användas som en del av den totala säkerhetslösningen för att skydda känslig information och övriga resurser.

En grundläggande segmentering av nätverket ligger i att skilja interna nät från Internet, samt att utvecklings-, test- och produktionsmiljöer ska vara skilda från varandra. Ytterligare segmentering ska göras då det är motiverat av säkerhetsskäl. Brandväggar och utrustning för segmentering av nätverk behöver revideras regelbundet för att hållas uppdaterade med rätt regler för kommunikation mellan olika IT-resurser över de olika nätsegmenten.

Krav

- ✓ Krav på skydd vad gäller nätverkstjänster ska identifieras, dokumenteras och tillämpas samt inkluderas i avtal för nätverkstjänster om dessa tjänster tillhandahålls som outsourcade tjänster.
- ✓ Trådlös datakommunikation innehållande information med normala eller **höga skyddskrav** avseende konfidentialitet är endast tillåtet från godkända klienter. Teknik för att kryptera och säkra kommunikationen (minst WPA2 PSK) ska alltid användas oavsett skyddskrav.
- ✓ En grundläggande segmentering av nätverket ska göras för att skilja interna nät från Internet, samt att skilja utvecklings-, test- och produktionsmiljöer från varandra. Grupper av informationstjänster, användare och informationssystem kan ytterligare segmenteras i separata nätverks efter skyddsbehov.
    - Utrustning ska finnas för att kontrollera och förhindra obehörig nätverkstrafik mellan olika nätverkssegment.
    - Dokumenterade kommunikationskontrakt ska upprättas mellan ägare för samtliga IT-resurser med kommunikation mellan olika segment. Kontrakten ska innehålla detaljerad information om vilka IT-resurser som ska kommunicera och vilka nätverksprotokoll och portar som ska användas. Kontrakten ska förnyas årligen och rutin ska finnas för att uppdatera regelverket för kommunikation mellan segment baserat på dessa kontrakt.
- ✓ Brandväggar ska konfigureras i enlighet med dokumenterad brandväggsrutin. Av brandväggsrutin ska framgå vilka nätverkstjänster som ska tillåtas, vilka händelser och aktiviteter som ska loggas och följas upp. Brandväggar och brandväggsrutin ska revideras periodiskt.
- ✓ Kommunikationstjänster mellan Hedemora kommun och externa nätverk ska dokumenteras och godkännas av IT-chef innan inkoppling får ske.

Informationsöverföring (ISO 27002 13.2)

Information som hanteras genom elektronisk meddelandehantering ska ges lämpligt skydd. Om e-post innehållande information med höga skyddskrav avseende konfidentialitet ska sändas till extern part ska lösning med kryptering och signering användas.

Avtal som reglerar säker överföring av verksamhetsinformation mellan Hedemora kommun och extern part ska upprättas. Användandet av osäkra klartextprotokoll såsom t.ex. FTP och HTTP ska undvikas och ersättas av säkra alternativ om information med normala eller **höga skyddskrav** avseende konfidentialitet ska överföras.

Krav

- ✓ Kommunikation med höga skyddskrav avseende konfidentialitet och riktighet ska alltid krypteras och kommunicerande parter ska identifieras på ett säkert sätt med digitala signaturer eller motsvarande.
- ✓ Utgående massutskick av e-post ska begränsas för att förhindra att kapad mailbox används till att skicka ut stora mängder spam.
- ✓ Överföringslösningar för verksamhetsinformation mellan Hedemora kommun och externa parter ska regleras genom avtal där minst följande regleras:
    - Motparten informeras om informationens klassning och garanterar att information med normala eller **höga skyddskrav** avseende konfidentialitet ges rätt nivå av skydd och inte förs vidare till annan part.
    - Kommunikationslösning ska definieras med de nätverkskomponenter som ingår i säkerhetslösningen samt den konfiguration och de inställningar som krävs för att upprätthålla rätt nivå av skydd.
    - Vid kommunikation med annan part med normala eller höga skyddskrav avseende konfidentialitet ska överföringen skyddas med kryptering
    - Trafik i uppsatta förbindelser ska loggas av båda parter.
- ✓ Kommunikation med e-post till andra organisationer skyddas i samtliga e-postsystem genom att konfigurera och aktivera standardiserade säkerhetsfunktioner och krypterad SMTP över TLS.

Anskaffning och utveckling av IT-resurs (ISO 27002 kap 14)

Korrekt informationssäkerhet för resurs ska säkerställas över hela livscykeln och börjar vid anskaffning eller utveckling.

Säkerhetskrav på IT-resurs (ISO 27002 14.1)

Krav som rör informationssäkerhet ska redan från början inkluderas i kraven för nya resurs likväl som i krav för förbättringar av befintliga. Det gäller oavsett om resurs upphandlas externt, utvecklas internt eller en kombination av båda (t.ex. anpassning av ett inköpt standardsystem).

Informationssäkerhetskraven ska spegla den klassning som tilldelats resurs och som baseras på t.ex. författningar och interna regelverk, riskanalyser eller analys av incidenter.

Utveckling, anskaffning eller förändring av system som omfattas av verksamhetsnära förvaltning ska involvera parterna i förvaltningsorganisationen. Informationsägare ansvarar för att rätt tekniska krav formuleras som överensstämmer med verksamhetens krav så att system ges skydd som korrelerar till klassningen.

Utveckling, anskaffning eller förändring av underliggande resurs i form av infrastruktur, stödsystem m.m. ska ha minst motsvarande krav som de system som de stöder. Ibland kan

kraven vara ännu högre än för de system de stödjer, exempelvis om en IT-resurs stödjer ett stort antal system som var för sig inte är kritiska.

Informationssäkerhetskrav ska dokumenteras och granskas av alla berörda parter innan utvecklingen, anskaffningen eller förändringen påbörjas.

Krav

- ✓ Informationssäkerhet ska inkluderas i kraven för nya resurs i förändringar av befintliga. Det gäller oavsett om IT-resursen upphandlas externt, utvecklas internt eller en kombination av båda (t.ex. anpassning av ett inköpt standardsystem). Informationssäkerhetskraven ska baseras på den klassning som tilldelats resurs och ska dokumenteras och granskas av alla berörda parter innan utvecklingen, anskaffningen eller förändringen påbörjas.

Säkerhetskrav vid upphandling av IT-stöd (ISO 27002 14.1)

Det är än viktigare vid extern upphandling att vara tydlig när det gäller kravställning av informationssäkerhet. Externa leverantörer använder kanske annan terminologi och har annan förståelse för informationssäkerhet än vad som föreligger internt i kommunen. Exempelvis är man kanske inte familjär med klassning av information och resurs, och även om man är det kanske man tillämpar andra nivåer och tolkar de olika nivåerna på annat sätt.

Avtal med IT-leverantör ska reglera ansvar för implementation och upprätthållande av säkerhetsfunktioner och ansvar för testning och verifiering av dessa. Dessutom ska avtalet reglera ansvar för sådana brister som eventuellt upptäcks under drift.

Om upphandlade system även ska driftas hos en leverantör tillkommer krav som kan innefatta:

- Fördjupade krav på leverantörens interna IT-miljö och informationssäkerhet (t.ex. certifieringar)
- Leverantörens kontinuitetshantering
- Rätt till tredjepartsrevision
- Sekretessavtal
- Personuppgiftsbiträdesavtal
- Rätt till incidentrapporter från leverantören.

I kravspecifikationer ska alltid tydliga krav på säkerhet formuleras som sedan används vid utvärdering av anbud. För att säkerställa en bra grund för att ta fram kravspecifikationer ska SKR:s KLASSA användas.

Upphandling av IT-stöd ska alltid göras i samverkan med Upphandlingscentrum. Hedemora kommun kommer att ta fram kravkataloger som baseras på hur resurs är klassade (se avsnitt B6 – Leverantörsrelationer).

Krav

- ✓ Tydliga informationssäkerhetskrav ska ställas vid upphandling av IT-stöd och ska sedan användas vid utvärdering av anbud. Kraven ska baseras på den klassning som tilldelats IT-resursen.
- ✓ IT-leverantörer ska alltid delge hur de bedriver säkerhetsarbete i såväl den operativa verksamheten som avseende säker systemutveckling.

- ✓ Avtal med IT-leverantör ska innefatta stöd och support i händelse av fel och incidenter.
- ✓ Avtal med IT-leverantör ska reglera hur kontroll av avtalets uppfyllande ska ske, t.ex. genom tredjepartsrevision eller granskning genomförd av Hedemora Kommun.
- ✓ Upphandling av system som ska driftas hos extern leverantör medför ytterligare krav, exempelvis:
    - Fördjupade krav på leverantörens interna IT-miljö och informationssäkerhet (t.ex. certifieringar)
    - Leverantörens kontinuitetshantering
    - Rätt till tredjepartsrevision
    - Sekretessavtal
    - Personuppgiftsbiträdesavtal
    - Rätt till incidentrapporter från leverantören
- ✓ Upphandling av IT-stöd ska göras i samverkan med Upphandlingscenter i Ludvika.
- ✓ Avtal med IT-leverantör ska innefatta:
    - Att leverantören innan leverans till Hedemora kommun genomför säkerhetstestning av system och ingående komponenter.
    - Att testet om möjligt genomföras av tredje part.
    - Att leverantören ska åtgärda eventuella säkerhetsbrister som identifierats i samband med acceptanstest och/eller leveranskontroll.
- ✓ Om IT-leverantör använder underleverantör för hela eller del av leveransen ska ett avtal tecknas dem emellan som reglerar såväl affärsmässighet som säkerhet. Avtalet ska kunna delges. Följande punkter ska då minst beaktas avseende säkerhet:
    - Hur applicerbara krav i avtal med IT-leverantör säkerställs även mot dess underleverantör.
    - Hur rättsliga krav uppfylls, exempelvis rörande lagstiftning om sekretess och personuppgifter.
    - Vilka åtgärder som vidtas för att säkerställa att alla berörda parter, inklusive underleverantörer, är medvetna om sitt säkerhetsansvar. licensieringsarrangemang, äganderätt till koden och upphovsrätt
    - Vilka åtgärder som vidtas för att säkerställa kvalitet i leverans från underleverantör.

Säkerhet vid systemutveckling (ISO 27002 14.2)

Systemutveckling är normalt ingen som vi ska hålla på med utan det ska vi uppdra åt våra leverantörer av IT-resurser att utföra.

Processer och rutiner ska finnas på plats för att säkerställa att informationssäkerhet designas och införs under utvecklingscykeln av IT-resurser. Säkerhet måste vara en integrerad del i utvecklingsprocessen, från början till slut. Regler för säker utveckling av program och system ska upprättas och tillämpas vid systemutveckling.

För systemutvecklings- och integrationsåtgärder ska utvecklingsmiljöer upprättas och skyddas över IT-resursens hela livscykel. En säker utvecklingsmiljö inkluderar människor, processer och teknik som är involverad i systemutveckling och integration. Det innebär även att alla utvecklare måste ha en grundkompetens i programvarusäkerhet och att utvecklingsprocesser innehåller komponenter av utbildning och omvärldsbevakning.

Outsourcad systemutveckling ska övervakas och styras och säkerhetsfunktionalitet ska säkerställas vid utveckling. En fördel är om leverantören använder en etablerad modell för

utveckling av säker programvara. exempelvis Microsofts Security Development Lifecycle (SDL), IBM:s The IBM Secure Engineering Framework eller OWASP (Open Web Application Security Project. Dessa modeller kan användas i kravställningen runt utvecklingsprocesser beroende på vilken metod utvecklingsleverantören använder. Om ingen etablerad modell används av leverantören krävs en betydligt mer ingående analys för att säkerställa en säker utvecklingsprocess.

Krav

- ✓ Processer, rutiner och regler ska finnas som reglerar att informationssäkerhet finns med under hela utvecklingscykeln av resurs.
- ✓ För systemutvecklings- och integrationsåtgärder ska utvecklingsmiljöer upprättas och skyddas över IT-resursens hela livscykel.
- ✓ Systemutvecklare ska ha kompetens i programvarusäkerhet.
- ✓ Vid outsourcad systemutveckling ska krav ställas att man tillämpar en etablerad modell för säker systemutveckling.

Säkerhetskrav vid test (ISO 27002 14.3)

Säkerhetsfunktionalitet ska testas vid utveckling och testning ska göras gentemot de ställda säkerhetskraven och i enlighet med riktlinjer för säker utveckling. Vid test kan man dra nytta av automatiserade verktyg, t.ex. verktyg för kodgranskning eller för skanning av sårbarheter. Testning bör utföras i en realistisk testmiljö för att säkerställa att systemet inte kommer att införa sårbarheter i organisationens miljö och att testerna är tillförlitliga.

Testdata bör skyddas och kontrolleras. System- och acceptanstest kräver normalt avsevärda mängder testdata som är så snarlika produktionsdata som möjligt**. Att använda produktionsdatabaser för test bör undvikas och personuppgifter måste i så fall först anonymiseras.**

Test-, utvecklings- och driftmiljöer ska separeras för att minska risken för obehörig åtkomst eller ändringar i produktionsmiljön. Utvecklare ska inte tillåtas att testa icke fastställda och godkända programversioner eller förändringar i driftmiljö.

Krav

- ✓ Säkerhetsfunktionalitet ska testas vid utveckling och testning ska göras gentemot de ställda säkerhetskraven och i enlighet med riktlinjer för säker utveckling.
- ✓ Produktionsdata ska inte användas i test utan all testdata ska väljas ut noggrant, skyddas och styras. Om produktionsdata ändå behöver används gäller följande:
    - o Testdata ska alltid anonymiseras från personuppgifter.
    - o Rutiner för styrning av åtkomst som tillämpas för produktionssystem ska också gälla vid test av sådana system.
    - o Behörighet ska godkännas av resursägare IT varje gång produktionsdata kopieras till ett testsystem.
    - o Produktionsdata ska omgående raderas från testsystem efter avslutad test.
    - o Kopiering av produktionsdata ska loggas för att erhålla spårbarhet.
- ✓ Test- eller utvecklingsversioner får ej placeras i produktionsmiljö utan utvecklings-, test och driftmiljöer ska separeras för att minska risken för obehörig åtkomst eller ändringar i produktionsmiljön.

Leverantörsrelationer (ISO 27002 15.2)

Informationsägaren ska årligen tillse att genomförs kontroll av de tjänster som leverantörer tillhandahåller. Tillsynen utgår från upprättade avtal. Alla typer av avvikelser ska dokumenteras och beroende på allvarlighet skyndsamt påtalas för leverantören.

Exempel på punkter som kan kontrolleras vid kontroll:

- Avtalstid på avtalet
- Nertid
- Svarstider på supportärenden.
- Kontroll av loggning
    - Vad har leverantören gjort för något under året?
    - Vad har Förvaltaren i systemet som kan vara konstigt?
- Kontroll av lagrad information hos leverantören.
- Incidenter som ev har inträffat.
- Leverantörens syn på utveckling IT-resursen.
- Etc.

Incidenthantering (ISO 27002 kap 16)

Med informationssäkerhetsincident avses en händelse som har eller skulle kunnat ha försämrat konfidentialitet, riktighet eller tillgänglighet hos information.

Alla medarbetare i Hedemora kommun är skyldiga att rapportera incidenter. Detta innefattar även externa aktörer som exempelvis konsulter. Även svagheter i skydd (brister) ska rapporteras, exempelvis larm som inte fungerar, öppna dörrar till våra lokaler eller öppna fönster efter kontorstid osv. IT- och informationsrelaterade incidenter och brister ska rapporteras till säkerhetschefen.

Processer och rutiner ska finnas på plats för att säkerställa ett konsekvent och effektivt tillvägagångssätt för hantering av informationssäkerhetsincidenter inklusive kommunikation i samband med incidenterna. Dessa incidenter an vara av olika typer, exempelvis:

- Obehöriga har fått tillträde till kommunens lokaler.
- Obehöriga har kommit åt information.
- Dokument, till exempel publika rapporter, har ändrats felaktigt eller utan behörighet.
- Infektion av virus eller annan skadlig kod.
- Information som borde ha funnits arkiverad har försvunnit.
- IT-resurser missbrukas av medarbetare eller externa personer.

Viktiga aktiviteter i incidenthanteringsprocessen är:

- Mottagning av information om incidenten.
- Styrning av eventuella behov av omedelbara åtgärder. Dessa kan vara av temporär art tills en mer hållbar lösning kan komma på plats.
- Analys av orsaker till incidenten så att korrigerande och preventiva åtgärder kan vidtas.
- Återkoppling och kommunikation med dem som är påverkade av eller involverade i återhämtning efter incidenten liksom till den som rapporterat incidenten.

Säkerhetschefen leder hanteringen av incidenter i samverkan med berörda ägare av resurs. Vid incidenter relaterade till förvaltningsresurs ska samverka ske med relevanta roller i förvaltningsorganisationen.

Incidenter där brott eller misstanke om brott föreligger ska alltid polisanmälas och insamling av bevis m.m. ska inte göras utan samråd med polisen.

Medarbetare och deltagare i verksamheten som har upptäckt en incident eller svaghet där brott misstänks föreligga, ska inte själva försöka bevisa detta då det kan försvåra utredningar.

Kunskaper baserade på analyser av hanterade incidenter ska användas för att minska sannolikheten eller konsekvenser av framtida, liknande, incidenter. Kort sagt bör man lära av sådant som har inträffat så att man kan vidta åtgärder för att förhindra återupprepning. Vissa åtgärder kan behöva vidtas skyndsamt och i samband med att en incident inträffar.

Större incidenter ska sammanställas i incidentrapporter som respektive informationsägare ansvarar för att ta fram i samverkan med säkerhetschef. Mindre incidenter ska registreras och sammanställas och kan ligga till grund för kvantifiering och statistik.

Erfarenheter från inträffade incidenter, t.ex. genom incidentrapporter och statistik, ska ligga till grund för framtida beslut för att förbättra skyddet, t.ex. att investera i nya säkerhetslösningar.

Krav

- ✓ Det ska finnas en incidenthanteringsprocess på IT som omfattar informationssäkerhetsincidenter. Processen ska innefatta:
    - Mottagning av information om incidenten.
    - Styrning av eventuella behov av omedelbara åtgärder. Dessa kan vara av temporär art tills en mer hållbar lösning kan komma på plats.
    - Analys av orsaker till incidenten så att korrigerande och preventiva åtgärder kan vidtas.
    - Återkoppling och kommunikation med dem som är påverkade av eller involverade i återhämtning efter incidenten liksom till den som rapporterat incidenten.
- ✓ Större incidenter ska sammanställas i incidentrapporter som respektive informationsägare ansvarar för att ta fram i samverkan med säkerhetschef.
- ✓ Erfarenheter från inträffade incidenter, t.ex. genom incidentrapporter och statistik, ska ligga till grund för framtida beslut för att förbättra skyddet, t.ex. att investera i nya säkerhetslösningar.
- ✓ Medarbetare är skyldiga att rapportera informationssäkerhetsincidenter såväl som informations- och IT-relaterade brister i system eller tjänster.
- ✓ Incidenter där brott eller misstanke om brott föreligger ska alltid polisanmälas och insamling av bevis m.m. ska inte göras utan samråd med polisen. Medarbetare och deltagare i verksamheten som har upptäckt en incident eller svaghet där brott misstänks föreligga, ska inte själva försöka bevisa detta då det kan försvåra utredningar.

Krisorganisation och krishanteringsplan

En krishanteringsplan Kontinuitet- och driftsplan ska finnas som ska aktiveras vid händelse av allvarliga incidenter eller kriser i IT-miljön. Ansvarig för krishanteringsplanen är IT-chefen innehålla bl.a. resurser, kontaktpersoner hos leverantörer som kan vara behjälpliga och operativa steg att vidta under en allvarlig störning.

Kommunens krisledningsorganisation organiseras efter behov.

Minst en gång per mandatperiod ska en IT-relaterad övning/utbildning genomföras.

- ✓ Det ska finnas en krisplan på IT som ska aktiveras vid händelse av en allvarlig incident eller kris. Krisplanen ska bl.a. innehålla krisorganisation, kontaktpersoner och operativa steg att vidta under en allvarlig störning eller kris.
- ✓ Krishanteringsplanen ska testas och övas minst en gång per år inom IT-avdelningen och en gång per mandatperiod för hela kommunen.
- ✓ Identifierade brister och svagheter ska åtgärdas i syfte att ständigt förbättra krisplanen för IT.

Kontinuitetshantering (ISO 27002 kap 17)

Kontinuitetshantering innebär att man i en organisation systematiskt arbetar med att och skapa en god återhämtningsförmåga för kritiska verksamhetsprocesser och minimera konsekvenserna av störningar, avbrott och katastrofer. Arbetet innefattar att identifiera kritiska verksamhetsprocesser och dessas beroenden av stöd och resurser som t.ex. personal, lokaler och verktyg.

Resurs är ofta viktiga stöd för kritiska verksamhetsprocesser som ibland kan vara helt beroende av att det finns tillgängligt och fungerar som avsett. Kontinuitetshantering för IT är därför en viktig del i informationssäkerhetsarbetet för att minimera negativa konsekvenser vid allvarliga IT-relaterade incidenter eller avbrott. Syftet är att efter ett större avbrott så snabbt som möjligt återgå till normalläge och att konsekvenserna för verksamheten ska vara så små som möjligt, både under och efter avbrottet.

Detta innebär att det för resurs med höga skyddskrav avseende tillgänglighet måste finnas en beredskap för hur man hanterar avbrott – s.k. avbrottsplaner. Resursägare IT ansvarar för att avbrottsplaner finns på plats och att de motsvarar de krav som finns för resurs. Avbrottsplaner ska vara relaterade till incidenthanteringen och den övergripande krishanteringsplan som ska finnas på IT-avdelningen En viktig säkerhetsåtgärd för att skapa och bibehålla hög tillgänglighet är säkerhetskopiering.

Krav

- ✓ Det ska finnas avbrottsplaner för samtliga kritiska Resurs med höga skyddskrav avseende tillgänglighet.
- ✓ Övning och testning av avbrottsplaner ska genomföras och utvärderas regelbundet och identifierade brister samt svagheter åtgärdas med syfte att ständigt förbättra kontinuiteten för IT.
- ✓ Avbrottsplaner ska finnas tillgängliga för de medarbetare som ingår i aktiviteterna, men samtidigt utgör planerna information med högt skyddsvärde och förvaras skyddat så att de inte blir åtkomliga för obehöriga.

Granskning och kontroll

Granskning av IT-säkerhet för IT-resurser ska ske regelbundet för att kontrollera att inga uppenbara sårbarheter exponeras och att tillräcklig säkerhetsnivå upprätthålls. Sådan granskning kan t.ex. vara skanning av sårbarheter med automatiserade verktyg eller så kallade penetrationstester. Särskilt viktigt är det att genomföra kontroll och granskning av kritiska delar av IT-miljön som direkt eller indirekt stöder system med **höga skyddsvärden**, samt införande av nya IT-lösningar.

Sårbarheter och brister som upptäcks vid granskningar ska tas upp för åtgärdande i genomförandeplaner, t.ex. förvaltningsplaner. Akuta sårbarheter och brister ska åtgärdas omedelbart. Rapportering av större sårbarheter och brister ska ske till informationssäkerhetsrådet.

Krav

- ✓ Kritiska delar i IT-miljön som stödjer resurs med höga skyddsvärden ska regelbundet övervakas och granskas för att sårbarheter och brister ska upptäckas.
- ✓ Nya IT-lösningar ska vid minsta osäkerhet gällande säkerhetsförhållanden utsättas för tekniska granskningar av extern part (t.ex. penetrationstester).
- ✓ Sårbarheter och brister som upptäcks vid granskningar ska tas upp för åtgärdande i genomförandeplaner, t.ex. förvaltningsplaner. Akuta sårbarheter och brister ska åtgärdas omedelbart.
- ✓ Rapportering av större sårbarheter och brister ska ske till informationssäkerhetsrådet.
- ✓ Revision av hela eller stora delar av IT-miljön ska göras minst vartannat år. Innan granskning eller revision kan ske ska följande beaktas:
    - Behov på åtkomst till system och data inför granskning eller revision ska avtalas med resursägare.
    - Omfattningen av tekniska aktiviteter för granskning eller revision ska beskrivas för- och godkännas av Informationsägare.
    - Aktiviteter vid granskning eller revision begränsas om möjligt till skrivskyddad åtkomst av program och data.
    - Granskning som kan påverka tillgänglighet bör utföras under servicefönster eller vid sådan tidpunkt då påverkan på verksamheten är så liten som möjligt.
    - All åtkomst vid granskning eller revision ska övervakas och loggas.

Bilaga 1 Sammanställning för säker hantering av information.

Klassificering av informationen	Styrande förordningar och lagar	Elektronisk lagringsplats	Skydd	Godkänd elektronisk-kommunikation	Lagring av utskrifter	Pappers-kommunikation
Kvalificerat Hemlig	Säkerhetsskyddslagen	Enligt fastställd rutin	Tagg / Fysiskt skydd / Kod/Användarnamn / Lösenord	Saknas	Tagg / Fysiskt skydd / Kod / Förteckning / Kvittens	Enligt fastställd rutin
Hemlig	Säkerhetsskyddslagen	Enligt fastställd rutin	Tagg / Fysiskt skydd / Kod/Användarnamn / Lösenord	Saknas	Tagg / Fysiskt skydd / Kod/Förteckning / Kvittens	Enligt fastställd rutin
Konfidentiellt Hemlig	Säkerhetsskyddslagen	Enligt fastställd rutin	Tagg / Fysiskt skydd / Kod/Användarnamn / Lösenord	Saknas	Tagg / Fysiskt skydd / Kod / Förteckning / Kvittens	Enligt fastställd rutin
Begränsat Hemlig	Säkerhetsskyddslagen	Enligt fastställd rutin	Tagg/ Fysiskt skydd /Kod/Användarnamn/ Lösenord	Signe	Tagg / Fysiskt skydd / Kod / Förteckning / Kvittens	Enligt fastställd rutin
Mycket känslig information / Sekretessbelagd information	Hälso- och sjukvårdslagen, Patientsäkerhetslagen, SoL, LSS, NIS mfl.	Utsedda informationssystem. Ostrukturerat material sparas i låsta mappar	2-faktorinloggning / Kvalificerat lösenord	Får endast ske i användarsystem.	Närarkiv / Personligt aktskåp	Rekommenderad post
Känsliga - och extra skyddsvärda personuppgifter	GDPR, SoLPuL	Utsedda informationssystem. Ostrukturerat material sparas i låsta mappar	2-faktorinloggning	TrustedDialog	Närarkiv / Personligt aktskåp	Rekommenderad post
Öppen information/ Harmlösa personuppgifter	Inga begränsningar	Kan läggas upp på hemsidan eller sparas i gemensamma mappar.	Behörighetsstyrd via AD och tilldelningar	Outlook	Städat skrivbord	Vanlig post