Rutin för informationssäkerhet

Dokumenttyp	Rutin
Fastställd/upprättad	2023-09-20 av IT-chef Peter Jonsson
Senast reviderad	
Detta dokument gäller för	Kommunövergripande
Giltighetstid	Tills vidare
Dokumentansvarig	IT-chef
Dnr	2023-293

Rutin för informationssäkerhet 5
Inledning 5
Rutinens omfattning 5
Dispenser och undantag 5
Introduktion till informationssäkerhet 6
Termer och definitioner 6
Kapitel A Informationssäkerhet för medarbetare 9
Inledning 9
Övergripande regler 9
Medarbetares ansvar för informationssäkerhet 10
Skyldighet att rapportera incidenter och brister 10
Informationsklasser 11
Märkning av sekretessklassade handlingar och information 12
Personuppgifter 13
Allmänna handlingar och sekretess 14
Lösenord 14
E-post 15
Chatt/direktmeddelanden (Videomötesplattformar exv Teams) 15
Lagring och säkerhetskopiering 16
Mobila enheter 16
Skadlig kod 18
Internet och sociala media 19
Etiska riktlinjer 19
Rutiner vid användning av sociala medier 19
Spårbarhet och loggning 20
Säkert beteende 21
Kapitel B Styrning av informationssäkerhet 23
Inledning 23
Roller och ansvar 23
Dokumentstruktur 25
Informationsklassning 26
Ledningssystem för informationssäkerhet 29
Personalsäkerhet 30
Leverantörsrelationer 32
Efterlevnad och granskning 32
Kapitel C Verksamhetsnära informationssäkerhet 34

Inledning ... 34
Roller och ansvar ... 34
Behörighetshantering och loggning ... 36
Logghantering ... 37
Ändringshantering ... 37
Användarinstruktioner ... 38
Riskanalys ... 38
Incidenthantering ... 38
Kontinuitetshantering ... 39
Kontroll av IT-tjänst ... 40
Kapitel D Informationssäkerhet i IT-miljön ... 41
Inledning ... 41
Roller och ansvar ... 41
Hantering av tillgångar ... 42
Styrning av åtkomst ... 43
Identifiering och autentisering ... 44
Reglering av åtkomsträttigheter ... 45
Säkerhetsloggning ... 46
Kryptering ... 47
Fysisk och miljörelaterad säkerhet ... 47
Driftsäkerhet ... 49
Skydd mot skadlig kod ... 49
Säkerhetskopiering ... 50
Loggning och övervakning ... 51
Hantering av tekniska sårbarheter ... 51
Kommunikationssäkerhet ... 52
Nätverkssäkerhet ... 52
Informationsöverföring ... 53
Anskaffning och utveckling av IT-resurser ... 53
Säkerhetskrav på IT-resurser ... 53
Säkerhetskrav vid upphandling av IT-stöd ... 54
Säkerhet vid systemutveckling ... 55
Säkerhetskrav vid test ... 56
Incidenthantering ... 56
Krisorganisation och krisplan ... 58
Kontinuitetshantering ... 58

Granskning och kontroll 59

Rutin för informationssäkerhet

Inledning

Hjo kommuns informationssäkerhetspolicy redovisar kommunens mål och inriktning med informationssäkerhetsarbetet. Rutin för informationssäkerhet – kompletterar och förtydligar informationssäkerhetspolicyn.

Rutinens omfattning

Rutinens innehåller information och regler gällande säkerhet vid all hantering av information inom Hjo kommun. Varken policy eller rutin omfattar kommunala bolag.

Rutinen gäller inte för säkerhetsskyddsarbetet och de informationssäkerhetsaspekter som faller under säkerhetsskyddslagen (2018:585).

Dispenser och undantag

Ansökan om dispens/undantag från riktlinjerna ska ställas till kommunens informationssäkerhetsråd tillika kommunens ledningsgrupp (KLG). Dessa ärenden ska vara beredda innan de kommer till KLG för beslut, en beredning ska innehålla en RKA (Risk- och konsekvensanalys). Beslut om undantag fattas av kommundirektör tillsammans med KLG. Undantagen är alltid tidsbegränsade dock aldrig längre än 2 år. Vid behov av förlängning av undantag så ska ärendet beredas ånyo.

Struktur och läshänvisningar

Rutinen är fördelad i fyra kapitel, varje kapitel redogör för en målgrupp.

Kapitel	Innehåll	Primär målgrupp
A. Informationssäkerhet för medarbetare	Information och rutin för hur information ska hanteras i olika situationer	Alla medarbetare
B. Styrning av informationssäkerhet	Ansvarsfördelning för informationssäkerhet. Information och rutin för hur arbetet med informationssäkerhet ska bedrivas	Verksamhetsansvariga, informationsägare, IT-personal
C. Informationssäkerhet i verksamhetsnära förvaltning	Information och rutiner för informationssäkerhet i förvaltningsobjekt som t ex system eller systemgrupperingar	Informationsägare, systemansvariga, verksamhetschefer och/eller enhetschefer
D. Informationssäkerhet i IT-miljön	Information och rutiner för hur information och IT ska hanteras inom IT-miljön dvs IT- säkerhet	Chefer och medarbetare på IT-enheten samt samverkans IT-organisation i Skövde

Informationsklassning är en central del i kommunens arbete med informationssäkerhet och finns

genomgående i rutinen. Klassningen avgör en informations skyddsvärde och definierar skyddsåtgärderna. Kapitel B beskriver Hjo kommuns klassningsmodell, liksom allt arbete och dokumentation/ rutiner/ instruktioner etc. utgår detta utifrån den internationella standarden SS-ISO/IEC 27002.

Introduktion till informationssäkerhet

Informationssäkerhet handlar om att skapa och upprätthålla lämpligt skydd av information. Detta innefattar information i alla dess former (text, bild, ljud, 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 säkerhet i IT-baserad informations-hantering handlar informationssäkerhet alltså om all information, oavsett form. Detta inkluderar förutom i IT-system även pappersbaserad information och information som finns i våra huvuden.

Information och de resurser som används för att hantera information benämns informations-tillgångar. Informationssäkerhet utgörs av tre aspekter; att informationstillgångar ska vara konfidentiella, riktiga samt tillgängliga.

Konfidentialitet – Att informationen inte tillgängliggörs eller avslöjas för obehöriga

Riktighet – Att informationen är korrekt, aktuell och fullständig

Tillgänglighet – Att informationen är åtkomlig och användbar för behörig

Olika typer av händelser (incidenter), som kan vara avsiktliga eller oavsiktliga, kan försämra konfidentialiteten, riktigheten eller tillgängligheten hos informationstillgångar. Information kan på ett oönskat sätt till exempel stjälas, raderas, förändras, avslöjas för obehöriga eller göras otillgänglig. En viss informationstillgång 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 informations-säkerhet. Vad som är lämplig nivå av skydd för en viss informationstillgång beror på dessa krav, hot-bild, och i vilka situationer informationen hanteras – hur den lagras, bearbetas, kommuniceras osv.

Termer och definitioner

Termer inom Informations- och IT-säkerhet är beskrivna i tabell på kommande sidor.

Term	Definition
Autentisering	Verifiering av att en användare eller IT-resurs är den som den utger sig för att vara
Behörighet	Tilldelade rättigheter att använda information eller en IT-resurs på ett specificerat sätt
Data	Omtolkningsbar framställning av information på ett formaliserat sätt lämpligt för kommunikation, tolkning eller bearbetning
E-postbluff/ E-mail spoofing	En form av spam eller phishing, där kriminella avsändare förfalskar avsändarens e-postadress till en e-postadress som mottagaren litar på i syfte att orsaka skada i någon form
IKT	Informations- och kommunikationsteknik
Incident	Enskild eller flera oönskade eller oväntade hän-

	delser som har negativa konsekvenser för verksamheten
Information	Kunskap om objekt, såsom fakta, händelser, saker, processer eller idéer, inklusive begrepp, som inom ett visst sammanhang har en särskild betydelse
Informationsklassning	Att genom konsekvensanalys identifiera skyddsbehovet för en viss information
Informationssäkerhet	Bevarande av informationens konfidentialitet, riktighet och tillgänglighet
Informationssäkerhetsincident	Enskild eller flera oönskade eller oväntade informationssäkerhetshändelser som har negativa konsekvenser för verksamheten och dess informationssäkerhet
Informationssäkerhetspolicy	Organisationens viljeinriktning med informationssäkerhet uttryckt av organisationens ledning
Informationstillgång	En mängd information, definierad och hanterad som en enda enhet, så att den kan förstås, delas, skyddas och utnyttjas effektivt. Informationstillgångar har igenkännligt och hanterbart värde, risk, innehåll och livscykler
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
Konfidentialitet	Att information inte tillgängliggörs eller avslöjas till obehörig
Ledningssystem för informationssäkerhet (LIS)	Ett sätt för organisationens ledning att på ett systematiskt sätt styra arbetet med informationssäkerhet i syfte att planera, genomföra, kontrollera, följa upp, utvärdera och förbättra säkerheten i verksamhetens informationshantering
Mobila enheter	Lättportabla IT-resurser såsom bärbara datorer, mobiler, läsplattor m m
Molntjänst	Molnbaserad tjänst, (på engelska: cloud-based service) – tjänst som tillhandahålls via Internet från ett nätverk av servrar. I princip ska användaren inte behöva ha mer än en webbläsare och internetanslutning för att använda tjänsten
Outsourcing	Utläggning av delar av ett företags eller myndighets produktion eller annan verksamhet till

	ett annat företag
Riktighet	Att information är korrekt, aktuell och fullständig
Sekretess	Förbud att i offentlig verksamhet röja uppgifter muntligen eller genom utlämnande av allmän handling. Regler om sekretess finns i offentlighets- och sekretesslagen respektive offentlighets- och sekretessförordningen
Skadlig kod/program/Malware	En form av programvara som kriminella har skapat i syfte att infektera datorer och andra enheter. Detta kan t ex vara virus, trojaner, maskar, ransomware, spyware och adware
Spårbarhet	En tydlig härledning av utförda aktiviteter till en identifierad användare eller IT-resurs
Stark autentisering	Som stark autentisering räknas identifiering av en person och verifiering av personens autenticitet
Tillgänglighet	Att information är åtkomlig och användbar av behörig
Verksamhetskritiska system	Kritiska system som har klassats med höga krav på konfidentialitet, riktighet och/eller tillgänglighet

Kapitel A Informationssäkerhet för medarbetare

Inledning

Detta kapitel vänder sig till alla medarbetare vid Hjo kommun. Rutinerna gäller även extern personal som har åtkomst till Hjo kommuns information, exempelvis inhyrda konsulter. Rutinerna beskriver det ansvar man som medarbetare har vid hantering av information i Hjo kommun och vilka regler som gäller. Hjo kommun är en organisation med många skilda verksamheter. Kompletterande regler till rutinerna kan därför finnas lokalt. Avvikelser från dessa rutiner får dock aldrig göras utan särskilt tillstånd. Kontakta ansvarig chef vid osäkerhet om vad som gäller.

Övergripande regler

Följande regler är övergripande och sammanställer grundläggande informationssäkerhetskrav på medarbetare:

1. Medarbetare ska vara medveten om sin skyldighet att rapportera informationssäkerhetsincidenter och -brister i Hjo kommuns personuppgifts- (GDPR) eller informationshantering och IT-säkerhet. Detta ska göras till IT-supporten eller till närmaste chef
2. Du som medarbetare har ansvar att kontrollera informationsklass så att du kan vara säker på att informationen får rätt skydd
3. Det är otillåtet att dela på personliga konton. Varje individ måste kunna kopplas till och därmed kunna hållas ansvarig för sina handlingar. Delar du ditt konto så blir du ansvarig för den aktivitet som kan kopplas till kontot – oavsett om det var någon annan som utförde handlingen eller inte
4. Medarbetare ska bara öppna länkar eller bifogade filer i e-postmeddelanden från betrodda avsändare. Det absolut vanligaste sättet att sprida skadlig kod för att stjäla information eller sabotera är att lura användare att klicka på länkar eller öppna bifogade filer i e-post.
5. Medarbetare får inte använda e-postadresser med domännamnet hjo.se för privat bruk som registrering av ett privat konto i kommersiella tjänster. Sådan registrering kan medföra att Hjo kommun får krav på att teckna företagslicens för nyttjande av tjänsten.
6. Genom att låsa din dator (CTRL + ALT + DEL, Välj Lås) eller (Windowstangent + L) medverkar du till att skydda känsliga uppgifter mot obehörig insyn och förändring. Exempelvis när personer passerar eller går in till ditt arbetsrum. Detta ska du göra varje gång du lämnar din dator obevakad, även för korta stunder.
7. Hjo kommuns medarbetare ska följa svensk lag och kommunens interna rutiner vid internetanvändning.
8. Du som medarbetare har rätt till skydd för din kommunikation och ditt privatliv. Men vid allvarlig misstanke om illojalt eller brottsligt beteende kan det vara tillåtet för arbetsgivaren att ta del av själva innehållet inte bara i arbetsrelaterat material utan även i dina privata filer eller e-postmeddelanden som finns i kommunens IT-miljö. Chef har till ansvar att se till att du som medarbetare är medveten om detta.
9. Medarbetaren ska ha kännedom om och tagit del av de styrdokument som berör medarbetarens arbete. Dessa finns publicerade på Hjo kommuns intranät och/eller kvalitetsledningssystem eller dylikt. Chef ansvarar för att ge medarbetare en introduktion till de styrande dokument som gäller.
10. Under distansarbete behöver du som medarbetare ta stort eget ansvar för att skydda kommunens information mot obehörig åtkomst.

Medarbetares ansvar för informationssäkerhet

Information är en viktig resurs för Hjo kommun som är av stor betydelse för alla våra verksamheter. I kommunen hanterar vi varje dag mängder av information som handlar om allt vad vi gör, och rör till exempel förskolor, grundskolor, socialtjänst, hemsjukvård, stadsplanering, biblioteksservice, bygglov m m.

Information kan förekomma i olika former, den kan vara muntlig, skriftlig eller finnas i IT-system. Information är främst i form av texter, men även bilder, symboler, filmer och ljud utgör information. Viss information är känslig och måste skyddas från obehöriga att ta del av. Det handlar ofta om hänsyn till den personliga integriteten och för att undvika att enskilda individer kommer till skada men också om sådan information som skulle kunna skada organisationen eller samhället om den sprids. Det finns en hel del lagar och föreskrifter som kommunen måste leva upp till.

Privatpersoner, företag och andra har förväntningar och behov på att kommunen hanterar information på ett säkert sätt. Informationssäkerhet handlar om att skapa och upprätthålla lämpligt skydd för att motsvara dessa krav. Information behöver olika slag av skydd. Det kan vara tekniskt såsom en brandvägg i ett IT-nätverk, eller administrativt i form av regler (som dessa rutiner) eller fysiskt hur man skyddar utrymmen med dörrar, lås, skåp m m.

Även medarbetares kunskap och medvetenhet är ett nog så viktigt skydd, till exempel att arbeta på rätt sätt med pappersdokument och i IT-system och att vara försiktig med känslig information som till exempel känsliga personuppgifter. 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 Hjo kommuns informationssäkerhet beror därför på hur den enskilde medarbetaren hanterar informationen. Hjo kommun ställer krav på att medarbetare följer våra rutiner för informationssäkerhet. Chefer har ett ansvar att delge information och erbjuda utbildning i informationssäkerhetsfrågor till sina medarbetare.

Som anställd på Hjo kommun omfattas du av en straffsanktionerad tystnadsplikt. Denna tystnadsplikt gäller även efter att din anställning upphört. Grundlagsstadgat finns din rätt att offentliggöra uppgifter enligt meddelarfriheten, med de begränsningar som finns i offentlighets- och sekretesslagen. Om du är externt kontrakterad och har tillgång till känslig information ska du skriva under en tystnads- och sekretessförbindelse. En sådan förbindelse gäller även efter att avtalet upphört. Vid underlåtenhet att följa dessa rutiner för informationssäkerhet följer Hjo kommun gällande regler enligt lagar och avtal. Lagbrott polisanmäls.

Skyldighet att rapportera incidenter och brister

Alla medarbetare har skyldighet att rapportera informationssäkerhetsincidenter eller brister som misstänkts kunna medföra negativ påverkan på Hjo kommuns information. Det kan röra sig om t ex

- IT-angrepp/intrång
- Skadlig kod
- Oskyddad känslig information
- Personuppgiftsincidenter
- Brister i efterlevnad av dessa rutiner för informationssäkerhet

IT-, informationssäkerhets- eller personuppgiftsincidenter och brister ska rapporteras till IT-support/ helpdesk (0500-498501) eller Serviceportalen. Meddela även din chef. Medarbetare som har upptäckt incidenter eller svagheter där brott misstänks föreligga, ska dock inte själva försöka bevisa sådana då det kan försvåra framtida utredningar. Det är bra att dokumentera iakttagelser i samband med upptäckten av incidenten. Informationssäkerhetssamordnare sammanställer en incidentrapport

en gång per år som rapporteras till kommundirektörens ledningsgrupp och berörda verksamheter. Rapporten omfattar:

- Intrång och försök till intrång
- Brott mot lagstiftning och internt regelverk
- Incidenter som orsakar eller skulle kunna orsaka betydande avbrott eller störningar
- Konsekvenser och förslag till åtgärder efter intrång eller funktionsfel

Informationsklasser

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. I Hjo kommun finns fyra klasser för hur känslig informationen är och hur den får spridas: Öppen, Begränsad, Känslig-Sekretess eller Hög Sekretess. Dessa illustreras i nedan tabell.

Informationsklass	Behörighet/ spridning	Exempel
4 Hög Sekretess (Röd)	Endast ett mycket begränsat antal behöriga personer	Skyddade personuppgifter, information som om den hamnar i orätta händer medföra fara för liv och hälsa eller samhällsskada
3 Känslig-Sekretess (Gul)	Endast den som behöver informationen för att klara sin arbetsuppgift, särskild åtkomstbegränsning med god spårbarhet	Känsliga personuppgifter, integritetskänsliga (extra skyddsvärda) såsom personnummer och sociala förhållanden, information under pågående upphandling, skalskyddsritningar
2 Begränsad (Grön)	Normal åtkomstbegräsning med viss spårbarhet	Allmänna personuppgifter, allmänna offentliga handlingar, födelsedata (6 första siffrorna i personnummer YYMMDD)
1 Öppen (Vit)	Ingen åtkomstbegränsning	Handlingar utan direkta eller indirekta personuppgifter

Olika regler gäller för dessa fyra klasser vad gäller spridning och hantering av information:

- Öppen (Vit) information kan spridas fritt. Ibland krävs dock beslut för att öppen information ska publiceras, t ex på extern webbplats som www.hjo.se
- För Begränsad (Grön) information gäller normal åtkomstbegränsning. Grön information kan normalt spridas internt inom kommunen och externt. Grön är en markering att informationen kan innehålla personuppgifter
- För Känslig-Sekretess (Gul) information gäller särskilda åtkomsträttigheter och hanteringsregler. Om känslig information delas till extern aktör ska det finnas ett tydligt syfte med detta. Känslig information får bara delas till betrodda externa parter
- För Hög Sekretess (Röd) information gäller mycket begränsade åtkomsträttigheter och minimal spridning. Uppgifterna kräver ofta strikt manuell hantering och ska så långt det är

möjligt hållas borta från digitala miljöer. Uppgifter i denna klass kan om de sprids medföra fara för liv och hälsa för den som uppgifterna avser eller för en stor mängd individer.

Det finns dessutom information som är klassat högre än Hög sekretess (Röd), sådan information regleras av säkerhetsskyddslagstiftning. Observera att särskilda regler finns för hantering av sådan information, kontakta Hjo kommuns säkerhetsskyddschef.

Inom Hjo kommun är idag långt ifrån all information klassad enligt de fyra klasserna. Att klassa information på det här sättet är ett arbete som startades under 2022 och pågår fortfarande. Det viktigaste är att Känslig-Sekretess (Gul) och Hög Sekretess (Röd) information hanteras på rätt sätt. Det är bl.a. känsliga personuppgifter och sekretessklassad information. Om du är osäker på hur viss information ska klassas och hanteras så fråga din chef eller kommunens IT-chef tillika informationssäkerhetssamordnare.

Märkning av sekretessklassade handlingar och information

För att uppmärksamma personen som tar del av sekretessklassad information ska handlingar, fysiskt i pappersformat och digitalt, vara försedd med en så kallad *anteckning*, en stämpel som upplyser läsare av informationen om att den är sekretessklassad (Se bilden nedan för exempel). Detta gäller för känslig (Gul) och Hög (Röd) sekretess.

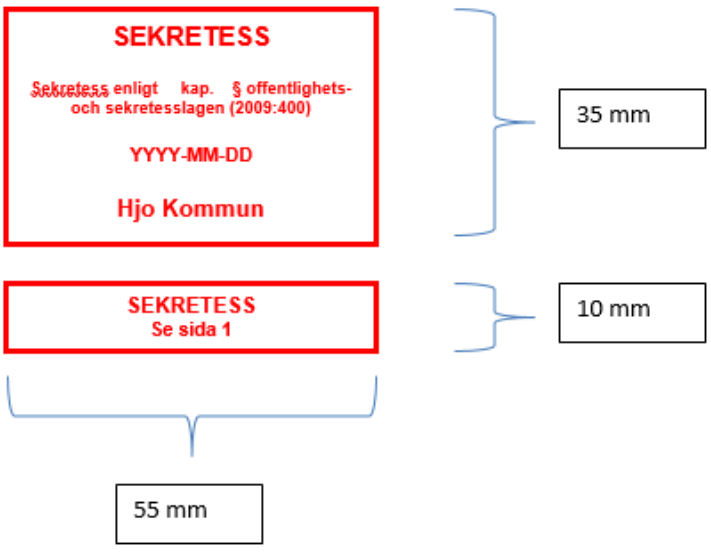
Vid överlämning eller delgivning av sekretessklassad information ska utlämnaren uppmärksamma mottagaren om sekretessklassningen.

Även lagringsmedia såsom USB-stickor, hårddiskar, CD-skivor eller dylikt ska vara märkta för att upplysa nyttjaren om det sekretessklassade innehållet. Lagringsmedia ska hållas under uppsikt eller inlåst om det inte används.

Anteckningen eller märkningen av handlingar, och lagringsmedia ska vara utformad på ett visst sätt för att styrka handlingens och klassningens *riktighet*.

Till höger visas hur sekretessmärkningen ska utformas. Utformningen är likadan för märkning av digitala och fysiska handlingar. Märkningen, stämpel eller digital, ska placeras på första sidan av den klassade handlingen. Om handlingen inte har ett försättsblad ska märkningen vara i sidhuvudet.

Om handlingen består av flertalet sidor ska samtliga sidor märkas. Till övriga sidor, förutom den första används den mindre märkningen och placeras i sidhuvudet.



Utöver placeringen ska märkningen också innehålla:

- Hänvisning till vilken lag, kapitel och paragraf man stödjer klassningen på
- Datum då klassningen utfördes
- Vilken myndighet/organisation som klassat handlingen (Alltid Hjo kommun för alla kommunens information)

Det är viktigt att vi i Hjo kommun kan styrka att vi tar hänsyn till offentlighetsprincipen och endast undanhåller allmänheten information med stöd av sekretessklassning som vi har legal rätt till. Offentlighets- och sekretesslagen är i de flesta val där vi hittar vad vi kan klassa som sekretess.

Personuppgifter

Vid de flesta av Hjo kommuns verksamheter hanteras personuppgifter. Dessa måste behandlas enligt gällande författningar bl. a EU´s dataskyddsförordning (GDPR) och Lagen om behandling av personuppgifter inom socialtjänsten. Personuppgifter kan vara klassade som Hög Sekretess (Röd), Känslig-Sekretess (Gul) eller Begränsad (Grön) information. Det beror på sammanhang, vilka personuppgifter som avses osv.

Känsliga personuppgifter är dock alltid lägst klassade som Känslig-Sekretess (Gul) information. Till känsliga personuppgifter räknas uppgifter som avslöjar:

- Ras eller etniskt ursprung
- Politiska åsikter
- Religiös eller filosofisk övertygelse
- Medlemskap i fackförening
- Genetiska uppgifter
- Biometriska uppgifter för att entydigt identifiera en fysisk person
- Uppgifter om hälsa
- Uppgifter om en fysisk persons sexualliv eller sexuella läggning

Utöver känsliga personuppgifter finns det också personuppgifter som Integritetsskyddsmyndigheten (IMY) kallar särskilt skyddsvärda. Detta är inte känsliga personuppgifter men uppgifter som IMY bedömt ändå kan orsaka stor skada ifall de inte hanteras korrekt.

För särskilt skyddsvärda personuppgifter gäller en högre teknisk säkerhet än för ”vanliga” personuppgifter. T ex får särskilt skyddsvärda personuppgifter inte skickas via okrypterad e-post utan det måste säkerställas att endast avsedd mottagare kan ta del av personuppgifterna.

Särskilt skyddsvärda personuppgifter klassas som Känslig-Sekretess (Gul) information. Exempel på särskilt skyddsvärda personuppgifter är:

- Personnummer
- Vissa löneuppgifter
- Uppgifter om lagöverträdelser
- Värderande uppgifter, till exempel uppgifter från utvecklingssamtal, uppgifter om resultat från personlighetstester eller personlighetsprofiler
- Information som rör någons privata sfär
- Uppgifter om sociala förhållanden

Skyddade personuppgifter är alltid Hög Sekretess (Röd) information och ska hanteras utifrån särskilda rutiner och regler. Fråga din chef om den verksamhet du arbetar i har särskilda rutiner för skyddade personuppgifter.

Allmänna handlingar och sekretess

En handling är allmän och ska registreras om den är förvarad, inkommen till, eller upprättad hos kommunen. Om handlingen omfattas av sekretess måste den diarieföras. Allmänheten ska kunna ta del av allmänna handlingar och kommunen är skyldig att, efter sekretessprövning, skyndsamt tillhandahålla den i läsbar form till den som så begär det. Allmänna handlingar kan vara både i form av analog och digital information och ska hanteras, bevaras och gallras i enlighet med verksamheternas dokumenthanteringsplaner. Information som är allmän handling och sekretessbelagd enligt offentlighets- och sekretesslagen ska klassas som Känslig-Sekretess (Gul) eller Hög Sekretess (Röd) information. Arbetsmaterial under ett ärendes beredning, minnesanteckningar, verksamhetsinterna meddelanden och personliga meddelanden är normalt inte allmänna handlingar. Denna information kan klassas som Hög Sekretess (Röd), Känslig-Sekretess (Gul), Begränsad (Grön) eller Öppen (Vit) information beroende på känslighet, t ex utifrån krav från författningar.

Lösenord

Regler för utformning av lösenord

1. Lösenord som du skapar för din inloggning till Hjo kommuns nätverk ska innehålla minst 1 stor bokstav, minst 1 liten bokstav, minst 1 specialtecken
2. Lösenordet får inte innehålla å, ä, ö, Å, Ä, Ö
3. Lösenordet får inte innehålla användarens inloggningsnamn, för- eller efternamn eller delar av namnet

Regler för hantering av lösenord

1. Lösenordet ska hanteras som en värdehandling och inte ligga framme uppskriven på en lapp. Bäst är att förvara lösenord endast i minnet. Behövs tekniskt stöd för att lättare hålla ordning på lösenord så kan man använda en så kallad lösenordshanterare. Det finns säkra och avgiftsfria lösenordshanterare på marknaden, kontakta IT - support för tips om sådana verktyg
2. Samma lösenord ska inte användas privat och i jobbet. Olika lösenord ska dessutom användas för olika tjänster på webben även om de är jobbrelaterade. På så vis minskas riskerna att någon kommer åt information
3. Lösenord ska bytas direkt om misstanke finns att det har röjts
4. Lösenord till ett personligt användarkonto får inte delas. Lösenord är personliga och ska inte delas mellan kollegor. Man kan i så fall bli ansvarig för något som någon annan har gjort. 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
5. Om en dator delas av flera är det viktigt att automatisk minnesfunktion för lösenordet inte används. Om man loggar in på webbsidor så ska man då inte låta webbläsare spara lösenordet, utan alternativet ”Nej” ska väljas om man får en sådan fråga. Webbläsare har funktioner för att i efterhand ta bort webbhistorik/ta bort lösenord, vilken kan användas om man är osäker på om lösenord har lagrats

För att logga in till de flesta av Hjo kommuns IT-system används användar-ID och lösenord. Lösenorden är personliga och får inte göras kända för andra. Om en obehörig kommer över ditt lösenord och får tillgång till ditt användar-ID, kan den personen utföra aktiviteter i ditt namn. Hamnar ett lösenord i orätta händer kan det orsaka stor skada. Användar-ID och lösenord används för att skydda information som kan vara intern eller konfidentiell, och det är därför viktigt att följa ovanstående regler för skapande och hantering av lösenord. 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.

E-post

Regler e-post

1. Din personliga brevlåda fornamn.efternamn@hjo.se är din tjänstebrevlåda
2. Den enskilde medarbetaren som är kontoinnehavare för ett personligt e-postkonto är alltid ansvarig för den mejl som skickas från kontot
3. E-postkonton kan stängas vid misstanke om brott eller missbruk
4. E-postkonton som delas av flera, t ex myndighetsbrevlådor (för nämnder) och funktionsbrevlådor (t ex för enheter) ska ha utpekade ansvariga
5. Mejl ska klassificeras enligt Hjo kommuns klassificeringsmodell. Skriv inte känsliga uppgifter i ämnesraden, eftersom inkorgens register över inkomna e-postmeddelanden räknas som allmän handling
6. Ska du skicka mejl till större grupper så ska du använda dig av funktionen ”Hemlig kopia”. Om du använder ”hemlig kopia” när du skickar mejl till större grupper undviker du att någon råkar skicka sitt svar till alla i gruppen trots att det bara var ämnat för dig som avsändare. Dessutom avslöjar du inte andras mejladresser om du använder ”hemlig kopia”
7. Om du får hotelsebrev via mejl ska du spara mejlet och kontakta din chef
8. Vid avslut av anställning tas e-postkontot bort efter viss tid, se därför till att mejl som din verksamhet kan behöva efter du har slutat din anställning sparas och lämnas över till annan handläggare
9. Håll isär arbetsrelaterad och privat kommunikation när du kommunicerar via e-post. Använd inte ditt epostkonto i Hjo kommun för privata ändamål, utan ha en privat e-postadress som du inte använder för arbetsrelaterat material
10. Det är inte tillåtet att automatiskt vidarebefordra din personliga e-postbrevlåda på kommunen till externa e-postadresser
11. Känslig – Sekretess (Gul) information får inte hanteras i Office 365 mejl
12. Information som klassificerats som Hög sekretess (Röd) får inte hanteras i Office 365 mejl
13. Om mejl inkommer som innehåller känslig - sekretess (gul) och Hög Sekretess (Röd) ska denna genast flyttas till verksamhetssystem. Svara inte avsändaren eller vidarebefordra ej i samma mejlkonversation, utan påbörja ny mejltråd utan känslig och sekretessinformation. Varpå meddelandet ska raderas från e-postklienten
14. Om mejl inkommer som innehåller Hög Sekretess (Röd) ska denna genast överföras till verksamhetssystem. Varpå meddelandet ska raderas från e-postklienten

E-post är för många medarbetare det vanligaste och viktigaste sättet att kommunicera internt inom kommunen och till externa parter. Det är dock viktigt att tänka på att kommunikation med mejl normalt är helt öppen. Att sända mejl som inte är skyddad, t ex med kryptering, kan jämföras med att skicka vykort.

Chatt/direktmeddelanden (Videomötesplattformar exv Teams)

Regler för chatt och känslig information

1. Känslig – Sekretess (Gul) information får inte hanteras i chatt
2. Information som klassificerats som Hög sekretess (Röd) får inte hanteras i chatt
3. Om chatt inkommer som innehåller känslig - sekretess (gul) och Hög Sekretess (Röd) ska mottagaren genast meddelas att känslig dialog på grund av säkerhetsskäl inte kan hållas per chatt. Hänvisa avsändaren till andra säkra kommunikationskanaler. Svara inte avsändaren

eller vidarebefordra ej i samma chattkonversation, utan påbörja känslig dialog i avsedda kommunikationskanaler. Varpå meddelandet ska raderas från chatten.

Chatt är för en del medarbetare ett vanligt och viktigt sätt att kommunicera internt inom kommunen och till vissa grupper av externa parter. Det är dock viktigt att tänka på att kommunikation med chatt normalt är helt öppen. Att sända chatt kan jämföras med att skicka vykort.

Lagring och säkerhetskopiering

Rutiner för lagring och säkerhetskopiering

1. Kommunens information ska lagras i kommunens tillhandahållna tjänster på så sätt att den finns tillgänglig för den som behöver den
2. Om information i undantagsfall behöver lagras på lokal hårddisk, se till att regelbundet kopiera över informationen till nätverket. Om hårddisken på din dator kraschar kommer annars informationen att vara förlorad
3. Om information på nätverket, exempelvis om man av misstag råkat radera ett dokument, ska IT-support kontaktas, förhoppningsvis kan de då återskapa den senaste säkerhetskopian
4. Känslig- Sekretess (Gul) information ska i första hand lagras i verksamhetssystem
5. Känslig- Sekretess (Gul) information får endast lagras i avsedda och godkända system och lagringsytor som har begränsad åtkomst, både vad gäller användare och administratörer av systemet eller lagringsytan
6. Hög Sekretess (Röd) information ska endast hanteras i verksamhetssystem om verksamhetssystemet har en tydlig funktion för sekretessmarkering. Saknar verksamhetssystemet stöd för detta får inte verksamhetssystemet hantera skyddade personuppgifter. Uppgifterna måste då vara fiktiva alternativt strikt hanteras utanför den digitala miljön
7. Lokal lagring (synkronisering) av Känslig – Sekretess (Gul) information, t ex på en persondator, får endast ske på en krypterad kommunägd dator
8. Lagring av Känslig – Sekretess (Gul) information på ett USB minne tillåts endast om informationen är rätt klassat och USB minnet är krypterat med krypteringsteknik som Hjo kommun tillhandahåller. Kontakta IT-support. USB minnet ska förvaras betryggande då det inte används
9. Fysiska dokument som innehåller Hög – Sekretess (Röd) information ska förvaras inlåsta på så sätt att uppgifterna endast är tillgängliga för den personal som behöver dem.

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

Rutiner för lagring i molntjänster

1. Endast godkända molntjänster är tillåtna att användas. Du ansvarar för att kontrollera vilka molntjänster som är tillåtna inom din verksamhet
2. Som användare ska du inte koppla en molntjänst du använder privat till din kommunala e-postadress
3. Hjo kommuns information får inte lagras i personliga molntjänster (Dropbox m fl)
4. Hög Sekretess (Röd) information får inte lagras i molntjänster

Mobila enheter

Den IT-utrustning som tillhandahålls av Hjo kommun kan vara stationär eller bärbar, en s.k. mobil enhet. Mobil enhet avser bärbar dator (laptop), USB-minne, CD/DVD-skiva, extern hårddisk samt smart telefon och surfplatta. Applikationsspecifika datorer, mobiler eller surfplattor kan ha specifika rutiner utöver dessa som presenteras här. Kolla med din chef om du är osäker vad som gäller.

Rutiner för hantering av mobila enheter

1. Känslig och sekretessinformation måste vara krypterad på mobila enheter
2. Mobila enheter ska låsas med lösenord eller liknande
3. Mobila enheter som tillhandahålls av Hjo kommun är personliga arbetsredskap och får inte lånas eller överlåtas om det inte är enheter som delas av flera
4. Uppsatta säkerhetsinställningar i enheter får inte ändras
5. Om du är i behov av ytterligare programvaror eller hårdvara ska du anmäla det till din närmaste chef
6. Viktig information bör inte lagras enbart på en bärbar enhet, i så fall ska den snarast kopieras över till kommunens nätverk så att informationen säkerhetskopieras
7. Privat utrustning kan anslutas till kommunens gästnät.
8. Kommunenheter får enbart anslutas till trådlösa nätverk som är betrodda och lösenordskyddade. Detta innebär att enheten inte får anslutas till ”öppna” nät till exempel på hotell, caféer, tåg eller flygplan
9. Vid distansarbete måste kommunens utrustning användas för kommunens information

Rutiner för fysisk hantering av mobila enheter

1. Försiktighet ska iakttas vid mobilt arbete i publika miljöer, exempelvis kan skärmen på enheten skyddas med insynsskydd (s.k. sekretesskydd)
2. Arbete med Känslig – Sekretess (Gul) och Hög sekretess (Röd) information får inte ske i publika miljöer.
3. Mobila enheter får inte lämnas utan uppsikt och ska förvaras i säkert och skyddat utrymme
4. Förlust av enhet ska omedelbart anmälas till IT-support, detta ska göras innan polisanmälan. I många fall finns möjligheter att fjärradera information
5. Vid avslut av anställning eller vid byte till en annan enhet ska mobila enheter återlämnas i enlighet med de rutiner som finns. I undantagsfall kan enheten behållas privat eller av en verksamhet, detta avgörs av närmaste chef tillsammans med IT-enheten
6. Utrustningen ska i övrigt vårdas och hanteras på det sätt som föreskrivs, t ex skyddas mot värme och fukt
7. Om utrustningen måste lämnas in för service så ska du försäkra dig om att den inte innehåller känslig eller sekretessinformation

Särskilda regler för smarta telefoner och surfplattor

Regler för smarta telefoner och surfplattor

1. Hjo kommun är som arbetsgivare ägare till de smarta telefoner och surfplattor som tillhandahålls för arbetet och även till den arbetsrelaterade informationen som finns i dessa enheter. Enligt offentlighetsprincipen kan det också vara möjligt för allmänheten att begära ut allmänna handlingar, till exempel arbetsrelaterade SMS eller bilder, som förvaras på telefonen/surfplattan
2. Det finns ett stort utbud av appar att ladda ner till den smarta telefonen eller surfplattan. Många av dessa appar kan innehålla skadlig kod.
3. Pinkod (6 siffror), fingeravtryck eller annan autentisering måste användas till smarta telefoner och surfplattor. Då pinkoder används ska ej enkla pinkoder som 000000, 123456 etc. användas, och inte samma pinkod som används i andra sammanhang, t ex pinkod till betalkort. Du får inte skriva upp koden på telefonen eller surfplattan
4. Vårda utrustningen och använd exempelvis skärmskydd och skal
5. Vid anställningens upphörande ska surfplatta och den smarta telefonen återlämnas till närmaste chef

6. Vid längre tjänstledighet kan telefonen behöva lämnas åter, det avgör närmaste chef
7. En smart telefon är ett viktigt verktyg för säker inloggning till kommunens IT-resurser som kräver multifaktorinloggning – därför måste din smarta telefon som arbetsgivaren tillhandahållit hanteras som en värdehandling.

Skadlig kod

Rutiner för skydd mot skadlig kod

1. Stäng aldrig av eller på annat sätt inaktivera installerat skydd mot skadlig kod
2. Anslut endast arbetsrelaterad IT-utrustning till kommunens administrativa nätverk
3. Var misstänksam och undvik att klicka på konstiga länkar eller fylla i kontouppgifter
4. Öppna bifogade filer endast om de kommer från en känd avsändare och en bilaga är förväntad. Är du osäker, ring avsändaren och fråga
5. Var observant på om IT-utrustning beter sig långsamt eller konstigt. Vid misstanke om skadlig kod, gör så här:
    a. koppla ifrån wifi/dra ur nätverkskabeln
    b. låt datorn vara på
    c. kontakta IT-support. OBS! Anmälan till IT-support ska ske per telefon eller besök, inte via e-post

Skadlig kod är ett samlingsbegrepp för oönskade datorprogram som virus, trojaner, spionprogram och maskar. Dessa kan installeras på en dator eller ett nätverk utan administratörens samtycke, och har utvecklats i syfte att störa IT-system, för att samla in information eller för att utnyttja datorkraft eller minneskapacitet i IT-utrustning. Skadlig kod är ett växande problem och den blir mer och mer sofistikerad och ”intelligent” och kan vara svår att upptäcka och kan utföra avancerade operationer. Man behöver idag inte vara en teknisk kunnig hacker för att skapa skadlig kod, utan det mesta kan köpas och beställas på olika marknadsplatser på Internet.

Exempel på idag förekommande skadlig kod:

- Ett ökande problem är s k Ransomware där filer eller diskar på dator (eller smart mobil eller surfplatta) krypteras och man sedan krävs på en lösensumma för att få tillbaka åtkomsten till filerna
- Vissa trojaner, s k keyloggers, kan avlyssna lösenord och skicka dessa vidare. Det finns trojaner som skapar bakdörrar i datorer så att andra personer får tillgång till dessa utan ägarens vetskap. Exempelvis med syfte att lagra olaglig information.

Spridning av skadlig kod

Skadlig kod kan spridas till ens dator eller mobila enhet om man öppnar bilagor i e-post, importerar filer eller surfar på Internet och klickar på fel länkar, inklusive sådana som finns i sociala medier. Avsändare till e-post kan fejkas och webbsidor är inte alltid de som de utger sig för att vara. Identiteter kan kapas, till exempel på Facebook, och e-postadresser kan fejkas i syfte att lura mottagaren att klicka på länkar. Vid s k Phishing luras mottagaren att klicka på en länk som leder till en sida där man ombeds fylla i koder, lösenord eller bankkonton. Var observant på detta och fyll aldrig i sådana uppgifter! Seriösa myndigheter, företag och andra organisationer ber aldrig om uppgifter på detta sätt. IT-utrustning som drabbats av skadlig kod, även ett smittat USB-minne, kan om det kopplas upp i kommunens nätverk, sprida sig vidare i nätverket och orsaka stor skada. Kommunens datorer är utrustade med skydd mot skadlig kod. Detta innebär inte fullständig säkerhet då utvecklingen inom detta område är oerhört snabb.

Internet och sociala media

Rutiner för internetanvändning

1. Internet är i arbetet på Hjo kommun främst ett arbetsverktyg och ska inte störa ordinarie arbetsuppgifter eller innebära merkostnader för kommunen
2. Det är tillåtet att använda Internet för privat bruk om det inte inkräktar på arbetet eller medför kostnader för kommunen. Kommunen förutsätter att den som surfar på Internet endast besöker lagliga webbplatser
3. Utrymmeskrävande filtyper inklusive filmer, program och spel får dock inte för privat bruk laddas ned, strömmas, lagras eller spridas i, eller via, Hjo kommuns nätverk
4. Det är inte tillåtet att via Internet titta eller lyssna på material av pornografisk karaktär. Förbudet gäller också material som är diskriminerande (religion, kön, sexuell läggning etcetera) eller har anknytning till kriminell verksamhet
5. De regler som gäller i samhället i övrigt gäller självklart även inom Hjo kommun. Tryckfrihetsförordningen, brottsbalken, lagen om upphovsrätt samt lagar som reglerar personuppgiftsbehandling är exempel på lagar som ibland måste beaktas när man använder Internet
6. 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
7. Internet är ett öppet nätverk och endast öppen information får publiceras, alltså inte Känslig - Sekretess (gul) eller Hög Sekretess (röd) information.

Användning av Internet och sociala medier kan vara till stor nytta och glädje, privat såväl som på arbetet. Förutom de rutiner som är kopplade till skadlig kod i ovan avsnitt finns här särskilda regler för användning av Internet och sociala medier.

Etiska riktlinjer

1. All kommunikation på Internet från Hjo kommuns datorer ska vara öppen, saklig och etisk, oavsett om kommunikationen sker för privata syften eller inte, eftersom kommunens enheter lämnar spår på Internet som leder tillbaka till vår organisation
2. 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. Uttalanden och andra aktiviteter som görs på Internet kan påverka allmänhetens uppfattning om den enskilde tjänstemannen som utför aktiviteten, och även för Hjo kommun som organisation. Det är därför särskilt viktigt att som representant för Hjo kommun beakta god etik och gott omdöme på Internet. Hjo kommuns etiska regler och värderingar ska följas även vid kommunikation via Internet och sociala medier.

Rutiner vid användning av sociala medier

1. Vid användning av sociala medier, se till så att det inte framstår som om åsikter som uttrycks är Hjo kommuns
2. Det är viktigt att du skiljer på vad du gör i sociala medier som privatperson och som representant för Hjo kommuns verksamheter.
3. Du har självklart rätt att diskutera Hjo kommun och jobbrelaterade saker som privatperson i sociala medier (förutom ärenden som omfattas av sekretess, se nedan). Ibland kan du behöva vara extra tydlig och förklara i vilken roll du uttalar dig eftersom du kan förknippas med din yrkesroll även på fritiden

4. Hemliga uppgifter får inte spridas och ärenden som berörs av sekretess eller tystnadsplikt får aldrig avhandlas i sociala medier, varken i privata konton, direktmeddelanden eller som inlägg i kommunens kanaler.
5. Gör du inlägg eller kommenterar med Hjo kommuns profil/användare så representerar du Hjo kommun. Skriver du med ditt eget namn och profil som avsändare gör du det som privatperson
6. I ditt personliga konto får du inte använda bilder och filmer som tillhör Hjo kommun utan att fråga fotografen först.
7. Hjo kommun är aktivt på sociala medier. Den personal som är utsedda att skriva i Hjo kommuns namn har särskilda regler och kunskap om kommunikation. Se vidare Hjo kommuns riktlinjer för sociala medier

Spårbarhet och loggning

Rutiner för granskning av loggar

1. Materialet får inte användas av arbetsgivaren i allmänt kontrollerande syfte
2. Misstanke om överträdelse ska vara väl dokumenterat. Dokumentationen ska innehålla beskrivning av händelsen, namn på person eller personer som gjort iakttagelser, datum, tidpunkt etc. Det är en förutsättning för att loggning skall kunna genomföras. Avsaknad av dokumentation innebär att loggning av enskild person inte får slås på

Rutin vid fördjupad granskning

Om det finns behov av fördjupad granskning av uppgifter på individnivå gäller följande:

1. Vid granskningen skall alltid två personer närvara
2. Verksamhetschef utser person från verksamheten och IT-chef utser teknisk assistans. Personerna får endast tillgång till loggarna i samband med granskningen
3. Granskningen ska genomföras skyndsamt och enligt fastställd teknisk rutin
4. Granskarna skall noggrant dokumentera anledningen till granskningen. I dokumentation skall det framgå vilka som genomfört den, samt datum, tid och plats för granskningstillfället

Gallring av loggar från granskning

Rutiner för gallring av loggar från granskning

1. Granskningsloggar ska raderas efter ärendet är avslutat
2. Undantag ska göras för loggar som påvisat brottslig aktivitet eller brott mot regler samt loggar som berörs av påbörjad undersökning. Sådan undersökning innebär att det material som då finns tillgängligt sparas och är tillgängligt till dess att undersökningen avslutats

Spårbarhet innebär att man genom loggning kan identifiera vem som har gjort vad och när och följa förloppet för olika händelser på datorn. All Internettrafik och e-post loggas centralt. Loggning sker i kommunens datorer och nätverk. Både filter och loggning är förenligt med GDPR. Loggarna används även för felsökning. Loggarna lagras under en viss tid, och är åtkomliga endast för en begränsad grupp administratörer. Hjo kommun kan, utan att meddela användaren, gå igenom dessa loggar för att kontrollera efterlevnad av lagstiftning och rutiner. Vid misstanke om brott kan loggfilerna komma att lämnas ut till rättskipande myndighet utan att du som kontoinnehavare meddelas.

Pornografi

Enligt detta styrdokument, som upprättats med stöd av kommunens informationssäkerhetspolicy, är det inte tillåtet att titta eller lyssna på material av pornografisk karaktär. Enligt brottsbalken är innehav av barnpornografi straffbart (brottsbalken 16:10a).

Illegal fildelning

Upphovsrätten innebär att den som skapat ett litterärt eller konstnärligt verk också har rätt till det. I den rätten ingår också att förfoga över verket genom att framställa exemplar av det och att göra det tillgängligt för allmänheten. Enligt upphovsrättslagen är det straffbart att dela ut den informationen till andra genom till exempel illegal fildelning. Förutom det personliga ansvaret riskerar den som medverkat till fildelning att bli skadeståndsskyldig till den som har upphovsrätt.

Rutin för loggning

GDPR medger rätt för arbetsgivaren, pga. allmänt intresse, att logga internettrafik utan personligt samtycke, med stöd av informationssäkerhetspolicy och för att säkerställa verksamhetens kontinuitet genom begränsande av internetanvändning för fildelning, kränkning/mobbning, rasism eller barnporr. Materialet får användas för att på ett strukturerat sätt beställa rapport på övergripande nivå (inte personrelaterad) där förbjudna sidor och på förhand definierade undersökningsområden fastställts. Sådana områden skall vara kända av personalen. Om det ur materialet kan påvisas att det skett slagningar mot förbjudna sidor eller frekvent användning på ett otillbörligt sätt kan verksamhetschef beställa fördjupad granskning av materialet.

Individuell loggning

Om det finns misstanke om överträdelse av regler eller misstanke om brottslighet kan verksamhetschef besluta om loggning av enskild persons användning av Internet eller

Internetanvändning för en grupp användare. Det innebär att samtliga lyckade internetsökningar loggas. Sparade loggar omfattar uppgift om vilken person som besökt adresserna. Direkt granskning av loggar får endast ske när det finns anledning misstänka att överträdelser sker.

Säkert beteende

Rutiner för muntlig information

1. Känslig – Sekretess (Gul) och Hög Sekretess (Röd) information har en begränsad krets av behöriga. Detta måste beaktas så att inte obehöriga kan höra sådan information på arbetsplatsen, både i arbetssituationer och 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
2. Känslig – Sekretess (Gul) och Hög Sekretess (Röd) information får överhuvudtaget inte kommuniceras muntligt i publika lokaler. Om man behöver behandla känslig information i kontakten med brukare i publika rum som till exempel bibliotek är det viktigt att föra samtalet på ett sådant sätt att risken för att känslig information sprids till obehöriga minimeras
3. Endast öppen information ska kommuniceras hörbart utanför arbetsplatsen, exempelvis vid fysiska samtal på tåget, eller i telefonsamtal i kassakön.

Rutiner för information på skärmar och i pappersform

1. Skriftligt material som innehåller Känslig – Sekretess (Gul) och Hög Sekretess (Röd) information får inte ligga framme så att obehöriga kan läsa den. Materialet ska låsas in i egen hurts eller eget skåp när man lämnar arbetsplatsen, även för kortare stunder
2. Känslig – Sekretess (Gul) och Hög Sekretess (Röd) information på datorskärmen ska vara skyddad från obehöriga. Skärmen ska låsas när man lämnar datorn, även för en kortare stund. Om man har ett s k smart kort till datorn (SITHS el likn) ska detta tas ut då man lämnar arbetsplatsen
3. Känslig – Sekretess (Gul) och Hög Sekretess (Röd) information ska skyddas från insyn med hjälp av sekretessfilter på datorskärm i de fall då sådan information hanteras på plats där

insyn från sidan kan ske. Sekretessfilter kan efter bedömning av närmaste chef tillhandahållas av arbetsgivaren

4. Besökare får inte vistas utan uppsikt i lokaler där Känslig – Sekretess (Gul) och Hög Sekretess (Röd) 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. Datorer i publika rum, till exempel bibliotek, med känslig information får inte lämnas utan uppsikt utan att låsas ner
5. Vid fysisk posttjänst ska dubbla förslutna brev (internpostkuvert och kuvert) användas för intern information och rekommenderade försändelser ska användas om externbrev innehåller Känslig – Sekretess (Gul) och Hög Sekretess (Röd) information
6. Fax är ett väldigt osäkert kommunikationssätt. Därför håller kommunen på att ersätta faxen med Säker Digital Kommunikation, lösningen ska införas under 2022. Om Känslig – Sekretess (Gul) information överförs via fax ska man försäkra sig om att man har 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.
7. Fax får inte användas till Hög Sekretess (Röd) information
8. Vid utskrift ska dokument omgående hämtas upp ur skrivare. Vid utskrift av Känslig – Sekretess (Gul) och Hög Sekretess (Röd) information måste så kallad Safe com printing (inloggning med passerkort) användas. Utskriften ska alltid övervakas så att man är säker på att ingen obehörig kan läsa informationen. Det ska också säkerställas att samtliga dokument är helt utskrivna innan man lämnar skrivaren.

Kapitel B Styrning av informationssäkerhet

Inledning

Detta kapitel beskriver och reglerar hur arbetet med informationssäkerhet ska bedrivas i Hjo kommun. Det beskriver också hur ansvarsfördelningen ser ut i stort. Ansvar för varje målgrupp återfinns också i varje kapitel, varför den övergripande ansvarsfördelningen i detta kapitel i huvudsak är informativ och ger en överblick över ansvaret för informationssäkerhet. Den primära målgruppen för detta kapitel är förutom informationsägare de som arbetar med informations- och IT-säkerhet eller har ansvar för informationssäkerhet i förvaltningsobjekt, projekt, processer eller andra verksamheter. Kapitlet kan även vara informativt för andra som är intresserade av hur arbetet med informationssäkerhet bedrivs i Hjo kommun, exempelvis sådana som arbetar med ledning och styrning av andra närliggande områden och processer som exempelvis kvalitet och annan säkerhet. I kapitlet ges en introduktion till informationsklassning och den modell för informationsklassning som Hjo kommun antagit i och med dessa rutiner.

Roller och ansvar

Grundprincip

Ansvaret för informationssäkerheten följer det ordinarie verksamhetsansvaret. Detta innebär att den som är ansvarig för en viss verksamhet (avdelning, enhet, process, projekt o.s.v.) också är ansvarig för informationssäkerheten inom verksamhetsområdet. Kommunens informations-säkerhetssamordnare, person-uppgiftssamordnare och övriga som arbetar specifikt med informationssäkerhet, IT-säkerhet eller andra relaterade frågor fungerar som stöd till medarbetare, verksamheter, kommunens ledning och nämnder för att de ska kunna ta ansvaret för informationssäkerheten.

Kommunfullmäktiges ansvar

Kommunfullmäktige fastställer övergripande mål och inriktning för informationssäkerhet genom en kommunövergripande informationssäkerhetspolicy.

Kommunstyrelsens ansvar

I kommunstyrelsens ledningsfunktion ligger att leda, samordna och utöva tillsyn gällande det kommunövergripande informationssäkerhetsarbetet. Kommundirektören har ansvar för att informationssäkerhetsarbetet bedrivs i linje med den av kommunfullmäktige fastställda informationssäkerhetspolicyn.

Ansvar inom varje verksamheter

Varje verksamhet är ansvarig för informationssäkerheten inom sitt verksamhetsområde. Verksamheten kan vid behov besluta om instruktioner som kompletterar de centrala rutinerna för informationssäkerhet. Verksamhetsansvarig, ansvarar för informationssäkerheten inom sin verksamhet. Verksamhetsledningen ansvarar för att verksamhetens medarbetare känner till och efterlever informationssäkerhetspolicyn och rutiner för informationssäkerhet.

Verksamhetsledningen ska visa sitt stöd för styrande processer för informationssäkerhet och fungera som förebild i informationssäkerhetsfrågor. Det åligger varje verksamhetsansvarig att se till att sina medarbetare har ett säkerhetsmedvetande och tillräcklig förståelse och kunskap för att en erforderlig informationssäkerhet i verksamheten kan uppnås. Säkerhetsansvaret i sig kan inte delegeras, däremot kan ansvaret att genomföra vissa arbetsuppgifter fördelas.

Medarbetares ansvar

Alla medarbetare inom verksamheten har ett ansvar för verksamhetens informationssäkerhet. Varje anställd ska i eget arbete följa rutiner för informationssäkerhet samt eventuella

verksamhetsspecifika regler. Varje anställd har även skyldighet att rapportera informationssäkerhetsrelaterade brister och incidenter. Om någon enskild befattningshavare ändå bryter mot gällande styrdokument bär vederbörande själv ansvaret för sitt handlande. Rutiner för medarbetare återfinns i Kapitel A.

Personuppgiftsansvar

Kommunstyrelsen är personuppgiftsansvariga. Som personuppgiftsansvariga har kommunstyrelsen det yttersta ansvaret för all behandling av personuppgifter och informationssäkerheten.

Om behandlingen sker i strid med dataskyddslagstiftning eller andra bestämmelser kan den personuppgiftsansvarige ställas till ansvar, oavsett om denne haft uppsåt att handla i strid med lagen eller varit oaktsam. Den personuppgiftsansvarige har också en skyldighet att kunna visa att man följer dataskyddsförordningen, t ex genom fastställda rutiner eller andra styrdokument. I enlighet med EU´s dataskyddsförordning och nationell dataskyddslagstiftning ska varje kommun utse ett dataskyddsombud. Den personuppgiftsansvarige ska säkerställa att dataskyddsombudet på ett korrekt sätt och i god tid deltar i alla frågor som rör skyddet av personuppgifter. Personuppgiftsansvarig ska också stödja dataskyddsombudet i utförandet av dennes uppgifter (som avses i artikel 39 GDPR) genom att tillhandahålla de resurser som krävs för att fullgöra dessa uppgifter samt tillgång till personuppgifter och behandlingsförfaranden. Hjo kommun har i samverkan med grannkommuner ett dataskyddsombud.

Systemägare

Systemägare ansvarar för att verksamhetssystemen efterlever informationssäkerhetspolicy och rutiner för informationssäkerhet. En viktig del i ansvaret är att besluta om verksamhetssystemens informationssäkerhetsnivåer genom att klassning sker i enlighet med Hjo kommuns modell för informationsklassning. Informationssäkerhetsansvar hos övriga roller inom Hjo kommun beskrivs i kapitel C. Rutiner för informationssäkerhet i verksamhetsnära förvaltning återfinns i kapitel C.

IT-enhetens ansvar

IT-enheten ansvarar för att kravställa den tekniska säkerheten på kommunens driftpartner Skövde IT-avdelning. Skövde kommun ansvarar för att leverera en IT-miljö som motsvarar IT-säkerhetsmässiga krav på tjänster, processer, system, infrastruktur, verktyg etc.. En IT-miljö som är robust, tillräcklig och uppfyller verksamheters krav, legala krav samt informationssäkerhetspolicyn och rutinerna för informationssäkerhet.

IT-chef (IT-säkerhetsansvarig/Informationssäkerhetssamordnare)

IT-chef samordnar arbetet med säkerheten i Hjo kommuns IT-miljö och som är stödjande vid kravställning på externa aktörer. Rollen IT-säkerhetsansvarig beskrivs utförligare i kapitel D.

Informationssäkerhetsarbetet i kommunen leds och samordnas av rollen informations-säkerhetssamordnare (IT-chef).

I detta ansvar ingår

- att kommunens styrande dokument inom området är aktuella, som informationssäkerhetspolicy och rutiner för informationssäkerhet,
- att utveckla och förvalta metoder, vägledningar och annat stödmaterial inom informationssäkerhetsområdet,
- kompetensförsörjning och att öka informationssäkerhetsmedvetandet inom kommunen, t ex genom rådgivning och utforma utbildning,
- att stödja verksamheterna i frågor som rör informationssäkerhet,
- att samordna/ stödja kommunens personuppgiftshantering
- kontroll och uppföljning av informationssäkerheten,

- omvärldsbevakning inom informationssäkerhetsområdet,

Säkerhetsstrateg

Hjo kommuns säkerhetsstrateg har uppdraget att utöva kommungemensam styrning av säkerhetsarbetet. Varje verksamhet ansvarar för säkerhets- och trygghetsarbetet inom sitt område.

Säkerhetsstrategen ska verka organiserande och koordinerande av kommunens säkerhetsarbete samt ska stödja verksamheterna och de kommunala bolagen i deras säkerhetsarbete.

Dataskyddsombud

Dataskyddsombudets uppgift är att informera och ge råd till den personuppgiftsansvariga och dess organisation om de skyldigheter som gäller enligt dataskyddsförordningen. Dataskyddsombudet ska också övervaka att dataskyddslagstiftningens och personuppgiftsansvariges strategi för skydd av personuppgifter efterlevs, detta inbegriper ansvarstilldelning, information och utbildning till personal och tillhörande granskning. Den personuppgiftsansvarige ska stödja dataskyddsombudet i dennes utförande av dessa uppgifter. Dataskyddsombudet ska på begäran ge råd om konsekvens-bedömningar avseende dataskydd och övervaka genomförandet av konsekvensbedömningen. Dataskyddsombudet ska samarbeta med tillsynsmyndigheten och vid behov fungera som kontakt-punkt för tillsynsmyndigheten. Dataskyddsombudet ska också fungera som kontaktperson för registrerade. Registrerade kan kontakta dataskyddsombudet i alla ärenden som har att göra med behandling av deras personuppgifter och utövandet av rättigheter med stöd av dataskydds-förordningen.

Kommunens revisorer

Kommunens revisorer utför kontroll av informationssäkerheten inom ramen för ordinarie revisioner.

Dokumentstruktur

Rutiner för dokumentstruktur för informationssäkerhet

- Hjo kommuns informationssäkerhet och dess behov ska analyseras i en informationssäkerhetsanalys. Analysen ska genomföras minst vart fjärde år och ska ligga till grund för hur arbetet med informationssäkerhet ska bedrivas och innehåll och utformning av övriga styrande dokument
- Årliga handlingsplaner för informationssäkerhet ska tas fram baserade på informationssäkerhetsanalyser
- Det ska finnas en för Hjo kommun övergripande informationssäkerhetspolicy som uttrycker ledningens viljeinriktning med informationssäkerhet
- Det ska finnas kommunövergripande rutiner för informationssäkerhet som konkretiserar informationssäkerhetspolicyn och som riktar sig till relevanta målgrupper
- Det ska finnas modeller, metoder, vägledningar och andra stöddokument som stödjer olika gruppers efterlevnad av informationssäkerhetpolicyn och rutinerna för informationssäkerhet

Det är fyra dokument som är centrala för kommunens arbete med informationssäkerhet:

- Informationssäkerhetspolicy
- Rutiner för informationssäkerhet (detta dokument)
- Informationssäkerhetsanalys (-er)
- Handlingsplan (-er) för informationssäkerhet

Informationssäkerhetspolicy och Rutiner för informationssäkerhet (detta dokument) riktar

sig till alla medarbetare inom Hjo kommun:

Informationssäkerhetspolicyn är ett övergripande dokument som uttrycker kommunstyrelsens

viljeinriktning med informationssäkerhet. Beslutas av Kommunfullmäktige och uppdateras vid behov.

Rutiner för informationssäkerhet (detta dokument) innehåller rutiner för hantering av information. Rutinerna är uppdelade i kapitel för olika målgrupper.

Informationssäkerhetsanalys och **Handlingsplan** för informationssäkerhet riktar sig främst till de som arbetar med styrning av informationssäkerhet i Hjo kommun:

- Informationssäkerhetsanalysen är en genomlysning av informationssäkerheten i Hjo kommun innefattande hotbild, skyddsnivåer, kommunens inriktning och interna och externa krav. Analysen genomförs i full skala vart fjärde år men justeringar kan göras löpande beroende på förändringar i kommunen eller externt. Informationssäkerhetsanalysen ligger till grund för hur arbetet med informationssäkerhet ska bedrivas och innehåll och utformning av de övriga dokumenten
- Handlingsplaner för informationssäkerhet tas fram årligen och innehåller konkreta mål och åtgärder baserade på informationssäkerhetsanalysen.

Lokalt, t ex i förvaltningar och i verksamheter, kan mer specifika instruktioner och vägledningar tas fram i syfte att komplettera eller förtydliga rutinerna för informationssäkerhet.

Informationsklassning

Rutiner för informationsklassificering

- Det ska finnas en kommungemensam modell för informationsklassificering
- Hjo kommuns modell för informationsklassning ska tillämpas för kravställning på informationssäkerhet genom att information ska klassas i enlighet med modellen och krav på säkerhetsåtgärder ska kopplas till de olika nivåerna i klassningsmodellen

Informationsklassning är en grundläggande komponent i informationssäkerhetsarbetet. Genom att klassa information utifrån krav på dess konfidentialitet, riktighet och tillgänglighet skapar man förståelse för, och kan styra vilket skydd som krävs för olika informationstillgångar. Främst handlar det om att skyddet ska bli tillräckligt, men ibland också för att undvika överskydd – med onödigt höga kostnader som följd. Klassning av information ska ske utifrån rättsliga krav som lagar och föreskrifter, men även interna krav på informationens värde, känslighet och betydelse för Hjo kommuns verksamheter. Att klassificera information på ett enhetligt sätt utifrån konfidentialitet, riktighet och tillgänglighet är en fundamental aktivitet i ett ledningssystem för informationssäkerhet (LIS) och ett krav i standarden SS-ISO/IEC 27001, vilken Hjo kommun avser att följa i dess informationssäkerhetspolicy. Det är också en rekommendation från MSB – Myndigheten för samhällsskydd och beredskap – att organisationer ska klassa sin information och bygga sina säkerhetsåtgärder utifrån klasserna. I den vägledande standarden SS-ISO/IEC 27002 rekommenderas att man ska ta fram en organisationsgemensam modell för informationsklassning. En sådan modell definierar nivåer av skyddskrav kopplat till de tre aspekterna konfidentialitet, riktighet och tillgänglighet så att information kan klassas på ett enhetligt sätt i hela organisationen. Hjo kommun har i och med dessa rutiner antagit en egen modell för informationsklassning. Modellen baseras på Sveriges nationella modell för informationsklassning som är utgiven av MSB och SIS, men har anpassats till kommunens behov.

Kravnivå	Konfidentialitet
3 Mycket höga skyddskrav	Hög sekretess – information som om den sprids till obehöriga kan medföra allvarlig negativ effekt för Hjo kommun, enskilda individer (fara för liv) eller andra organisationer
2 Höga skyddskrav	Känslig – Sekretess – Information som om den sprids till obehöriga kan medföra betydande negativ effekt för Hjo kommun, enskilda individer (fara för liv) eller andra organisationer
1 Normala skydds-krav	Begränsad information som om den sprids till obehöriga kan medföra måttlig negativ effekt för Hjo kommun, enskilda individer (fara för liv) eller andra organisationer
0 Inga skyddskrav	Öppen information som kan spridas fritt inom och utom Hjo kommun

OBS! Det finns dessutom information som är klassat högre än Hög sekretess (Röd), sådan information regleras av säkerhetsskyddslagstiftning.

Öppen information behöver alltså inte ha något skydd mot insyn och har normalt ingen begränsad åtkomst. Begränsad information behöver viss skydd av insyn då det ofta inbegriper personuppgifter. Däremot är det viktigt att förstå att all information – även Öppen och Begränsad – har minst normala skyddskrav när det gäller dess riktighet och tillgänglighet. Det kan också krävas beslut för att viss information ska vara öppen och publik. Idén med informationsklassning är att skydd ska anpassas till kraven på en viss informationstillgångs konfidentialitet, riktighet och tillgänglighet. En viss information kan exempelvis vara mycket kritisk när det gäller tillgänglighet och riktighet, men mindre känslig när det gäller konfidentialitet. Även hela IT-system klassificeras. När man då klassar enligt KLASSA metoden ska informationsvärdet bedömas utifrån alla tre aspekterna.

KLASSA nivå	
(4) Synnerligen allvarlig skada	Systemet behandlar information som omfattas av sekretess och rör Sveriges säkerhet (hemliga uppgifter) där röjande av information, felaktig information eller otillgänglig information kan ge oöverskådliga konsekvenser där t ex omfattande fara för liv och hälsa föreligger. Vid hantering av hemliga uppgifter ska Säkerhetsskyddslagstiftningen och Säkerhetsskyddsförordningen beaktas.
(3) Allvarlig skada	Skapar stora svårigheter för organisationens verksamhet. Omöjligt eller nästan omöjligt att fullfölja uppdragen. Samhällsviktiga funktioner i egen eller annan organisation påverkas sannolikt. Individers liv och hälsa äventyras. Känsliga personuppgifter kan ges stor spridning och orsaka allvarlig skada på den personliga integriteten.

(2) Betydande skada	Verksamheten kan fullfölja sina uppdrag, men med trolig risk för kännbar påverkan (ekonomiskt eller genom behovet av att vidta extraordinära åtgärder). Andra myndigheter och organisationer kan påverkas (ekonomiskt eller genom behovet av att vidta extraordinära åtgärder). Samhällsviktiga funktioner i egen eller annan organisation påverkas troligen inte. Enskilda individer kan uppleva konsekvenser, såsom stora besvär eller stor ekonomisk påverkan, av störningen. Personuppgifter kan spridas och orsaka betydande skada på den personliga integriteten.
(1) Måttlig skada	Inga märkbara större svårigheter för verksamheten att nå målen. Ingen påverkan på samhällsviktiga funktioner vid egen eller annan organisation. Enskilda individer eller andra myndigheter och organisationer kan notera störningen eller uppleva lindriga besvär men utan påvisbar ekonomisk påverkan. Enstaka personuppgifter av ej känslig karaktär kan komma att spridas och orsaka måttlig skada på den personliga integriteten.
(0) Försumbar skada	Inga svårigheter för verksamheten att nå målen. Ingen eller endast försumbar påverkan på samhällsviktiga funktioner vid egen eller annan organisation. Ingen eller försumbar skada på den personliga integriteten för enskild individ, vare sig avseende fysisk, ekonomisk eller integritetsrelaterad skada.

IT stödet får då en viss profil, t ex 1-2-2. Här är några exempel på hur det kan se ut när information klassats:

Informationsmängd	Konfidentialitet	Riktighet	Tillgänglighet
Öppettider stadshus	0	1	1
Personaluppgift	1	1	1
Patientjournal	2	3	3
Skyddade personuppgifter	3	3	3
Krisplan	1	3	3

Skyddsåtgärder kan sedan kopplas till de olika informationsklasserna. Olika typer av åtgärder kan användas för att uppfylla skyddskraven för de olika aspekterna. Exempel:

Kravnivå	Konfidentialitet	Riktighet	Tillgänglighet
Höga skyddskrav (3)	Kryptering, vid lagring och överföring. Stark inloggning.	Två-faktors autentisering, exempelvis SITHS kort, BankID eller Freja e-id	Spegling av databas, daglig säkerhetskopiering
Normala skyddskrav (1)	Inloggning med användarnamn och lösenord	Inloggning med användarnamn och lösenord	Regelbunden säkerhetskopiering

Vad ska klassificeras?

Det är informationen som är den primära tillgången och som ska klassas, och som sedan styr vilka skyddsåtgärder de olika nivåerna av skyddskrav medför. Resurser som används för att hantera informationen, t ex programvaror, tjänster och fysiska tillgångar, ska utformas och anpassas till de krav som klassningen i förlängningen ställer på dessa. IT-system ska klassas på grundval hur informationen är klassad som finns i eller hanteras av systemen. En viktig uppgift för systemägare/verksamhetschef är därför att klassa sina system så att rätt skyddskrav erhålls. Rutiner för detta finns i Kapitel C.

Informationsklassning har nyligen påbörjats i Hjo kommun, och långt ifrån all information är klassad. Målsättningen är främst att kritisk information ska klassas som har höga skyddskrav för en eller flera av aspekterna konfidentialitet, riktighet och tillgänglighet.

Användningsområden och målgrupper

Modellen vänder sig dels till de i Hjo kommun som är verksamhetsansvariga och/eller ägare av information och verksamhetssystem, dels till de som ansvarar för att rätt nivå av skydd skapas och upprätthålls. Den klassade informationen utgör ett underlag för en verksamhet vid kravställning av tjänster, exempelvis IT-tjänster, både internt och externt. Klassningsmodellen kan därigenom fungera som ett gemensamt ramverk och kommunikationsmodell vid förhandling mellan beställare och leverantör av tjänster. Identifiering och klassificering av information bör ske initialt när informationssäkerhetsbehovet ska analyseras men även som ett led i löpande förbättring eller vid förändringar av verksamheter eller IT-system. För de flesta medarbetare gäller endast aspekten Konfidentialitet, vilket betonas i kapitel A som riktar sig till alla medarbetare. Där illustreras en version av klassningsmodellen som endast innehåller aspekten konfidentialitet.

En mer utförlig vägledning som stöd för informationsklassning avses att skapas i framtiden.

Ledningssystem för informationssäkerhet

Rutiner för ledningssystem för informationssäkerhet (LIS)

I Hjo kommuns informationssäkerhetspolicy anges att man ska bedriva ett systematiskt informationssäkerhetsarbete. Med fördel baseras detta på standardserien SS-ISO/IEC 27000 med målet att skapa ett ledningssystem för informationssäkerhet (LIS). Ett LIS är ett etablerat begrepp för ett systematiskt arbete med informationssäkerhet och innebär en metodik som syftar till att upprätta, införa, driva, övervaka, granska, underhålla och förbättra organisationens informationssäkerhet. LIS avser här inte ett IT-baserat system, även om IT-stöd kan användas i delar av ett LIS. Eftersom kommunen och dess omvärld är i ständig förändring är informationssäkerhetsbehovet dynamiskt och måste ständigt anpassas till exempelvis organisationsförändringar, nya lagar, nya hotbilder och strömningar i samhället. Det räcker därför inte att skapa en skydd som svarar mot interna och externa förutsättningar idag, eftersom dessa kan se annorlunda ut i morgon. Ett systematiskt arbete med informationssäkerhet med ett LIS syftar i stort till att informationssäkerheten över tid anpassas efter interna och externa förutsättningar, och som därigenom upprätthåller en lämplig skyddsnivå över tid. I Hjo kommun har arbetet med att skapa ett LIS påbörjats i och med dessa rutiner där roller, ansvar och informationsklassning är viktiga element. Att planera och införa ett LIS kommer dock att fortgå under de närmaste åren. Tillsynsmyndigheter (Integritetsskyddsmyndigheten, IVO m fl) rekommenderar att kommuners informationssäkerhetsarbete och LIS utgår från standardserien SS-ISO/IEC 27000.

Standardserien innefattar en stor mängd standarder, men två standarder kan sägas utgöra seriens huvudstandarder:

- SS-ISO/IEC 27001 – Informationsteknik – Säkerhetstekniker Ledningssystem för informationssäkerhet – krav. Denna standard ställer som namnet antyder krav på ett LIS, dvs. vad det ska innefatta. I standardens bilaga A finns ett antal säkerhetsåtgärder som tjänar som utgångspunkt för vilka säkerhetsåtgärder som ska finnas
- SS-ISO/IEC 27002 – Informationsteknik – Säkerhetstekniker – Rutiner för informationssäkerhetsåtgärder. Denna standard ger vägledning för införande av säkerhetsåtgärderna i föregående standards bilaga A.

Dessa båda standarder är i Sverige och internationellt dominerande ramverk för styrning av informationssäkerhet. Sedan år 2009 är det exempelvis tvingande för svenska statliga myndigheter att tillämpa dessa enligt MSB:s föreskrifter och allmänna råd om statliga myndigheters informationssäkerhet (MSBFS 2016:1, tidigare MSBFS 2009:10). Standarderna i serien utgår från ett verksamhetsdrivet och riskorienterat arbete med informationssäkerhet, i motsats till ett teknikdrivet. Utgångspunkten är också att det är information som ska skyddas, utifrån de tre aspekterna konfidentialitet, riktighet och tillgänglighet, medan IT är sekundära resurser som används för att hantera informationen. Att standardserien är så etablerad och spridd innebär fördelar. Förutom att man tar tillvara samlade kunskaper och erfarenheter från hela världen så använder man ett gemensamt ramverk och en gemensam terminologi som underlättar vid kommunikation och samverkan med andra aktörer, exempelvis i samband med utbildning, revisioner och upphandlingar. Det finns även andra standarder i standardserien som framöver kan vara av intresse för Hjo kommun, exempelvis för mätning av informationssäkerhet (27004) och hantering av informationssäkerhetsincidenter (27035).

Ett LIS för Hjo kommun kommer att planeras och införas under ledning av IT-chef, arbetet startade under år 2020. Detta kommer att omfatta samtliga delar av informationssäkerhetsarbetet i kommunen.

Personalsäkerhet

Rutiner för personalsäkerhet före och i samband med anställning

- Bakgrundskontroll av sökande ska göras före anställning där sökandes meritförteckning verifieras
- Anställning av kritiska roller ska genomgå förstärkt kontroll i form av kreditupplysning och kontroll i brottsregister
- Befattningar som i Hjo kommuns säkerhetsskyddsanalys identifierats som säkerhetskänsliga ska vid rekrytering genomföra en säkerhetsprövning enligt säkerhetsskyddslagen (2018:585). En godkänd prövning är ett krav för anställning.
- Nyanställda ska via anställande chef delges ansvar och skyldigheter kopplade till informationssäkerhet och genomgå utbildning i informationssäkerhet samt ta del av informationssäkerhet för medarbetare enligt dessa rutiner. Och annat ansvar som följer med rollen, t ex informationsägarskap
- Anställda som får tillgång till sekretessinformation ska skriva på en sekretessförbindelse som används för att påminna om tystnadsplikten. Samtidigt ska den anställde informeras om meddelarfrihet

Rutiner för personalsäkerhet under anställning

- Alla medarbetare och i förekommande fall externa aktörer ska erhålla lämplig utbildning för att kunna efterleva kommunens informationssäkerhetspolicy och rutiner för informationssäkerhet

- Roller som har särskilda uppgifter inom informationssäkerhet ska får lämplig fortbildning inom området som är relevant för deras befattning
- Arbetsrättsliga åtgärder kan behöva vidtas då anställda har brutit mot gällande informationssäkerhetsregler

Rutiner för personalsäkerhet för avslut eller ändring av anställning

- Ansvar och skyldigheter för informationssäkerhet som förblir gällande efter avslut eller ändring av anställning ska definieras och kommuniceras vid anställningstillfället eller tillträdande av roll och framgå i sekretessförbindelse
- Återlämnande av IT-resurser och indrag av åtkomsträttigheter till information och IT-resurser ska ske i direkt samband med avslut eller ändring av anställning.
- Närmaste chef är ansvarig för att avbeställa behörigheter, passerkort, utrustning, smarta kort (SITHS) mm utifrån fastställda rutiner som gäller vid avslutning av anställning.
- När anställning avslutas ansvarar närmaste chef för att information som är av vikt för andra inom verksamheten lagras på annan lagringsplats än användarens OneDrive/Google Drive (Utbildning) m fl.

Personal är den viktigaste resursen i kommunen, och det är personal som dagligen hanterar information, manuellt eller med stöd av IT. Många roller kommer i kontakt med och hanterar kritisk och känslig information, och det är därför av största vikt att personalen får information och utbildning om informationssäkerhet, och att det finns rutiner i samband med anställning, förändring och avslut av anställning.

Före och i samband med anställning

Bakgrundskontroll av sökande till tjänster i Hjo kommun ska ske genom verifiering av sökandes meritförteckning, t ex genom kontakt med referenser och bekräftelse av påstådda akademiska och yrkesmässiga kvalifikationer. För vissa kritiska tjänster krävs en förstärkt kontroll i form av kreditupplysning och kontroll i brottsregister. Sådana kritiska tjänster är högre chefstjänster, säkerhetstjänster, eller för de som har åtkomst till känslig eller samhällsviktig information.

Lagsstiftningen om registerkontroll för skydd av barn och unga ska självklart efterlevas. För befattningar som har betydelse för rikets säkerhet, och således omfattas av Säkerhetsskyddslagen (2018:585), ska det i anställningsförfarandet genomföras en registerkontroll. Registerkontrollen ska genomföras innan en person genom anställning eller på annat sätt deltar i verksamhet som har betydelse för rikets säkerhet. De befattningar som är aktuella framgår av Hjo kommuns säkerhetsskyddsanalys och -plan. Registerkontrollen administreras av säkerhetsskyddschef. Alla bakgrundskontroller ska ta hänsyn till gällande lagstiftning rörande hantering av personuppgifter. Nyanställda ska delges ansvar och skyldigheter kopplade till informationssäkerhet och genomgå utbildning i informationssäkerhet samt ta del av informationssäkerhet för

medarbetare enligt dessa rutiner. Delgivning och utbildning ska också ges kopplat till annat ansvar som följer med rollen, t ex informationsägarskap. Alla anställda som får tillgång till sekretessinformation ska skriva på en sekretessförbindelse som används för att påminna om tystnadsplikten. Den anställde ska samtidigt informeras om sin rätt att offentliggöra uppgifter enligt meddelarfriheten, med de begränsningar som finns i offentlighets- och sekretesslagen. Den lagstadgade tystnadsplikten för sekretesskyddad information som den anställde får del av i tjänsten gäller även efter att anställningen upphört.

Under anställning

I enlighet med informationssäkerhetspolicyn ska medarbetare inom kommunen ha ett högt medvetande avseende informationssäkerhet. Alla medarbetare och i förekommande fall externa aktörer ska erhålla lämplig utbildning för att kunna efterleva kommunens informationssäkerhetspolicy och

rutiner för informationssäkerhet. Roller som har särskilda uppgifter inom informationssäkerhet, t ex inom IT-säkerhet eller förvaltningsorganisationen, ska få lämplig fortbildning inom området som är relevant för respektive befattning. Om anställda bryter mot gällande informationssäkerhetsregler ska dessa ärenden hanteras individuellt av ansvarig chef med stöd från personalfunktionen på samma sätt som vid andra ärenden gällande misskötsamhet.

Avslut eller ändring av anställning

Vid avslut eller ändring av anställning kan ansvar och skyldigheter för informationssäkerhet förbli gällande, exempelvis sekretessförbindelse och tystnadsplikt om den anställde haft tillgång till konfidentiell information. Detta ska definieras och kommuniceras till den anställde vid anställning/tillträdande av roll och framgå i sekretessförbindelsen.

Återlämnande av IT-resurser och indrag av åtkomsträttigheter till information och IT-resurser ska ske i direkt samband med avslut eller ändring av anställning.

Leverantörsrelationer

Rutiner för leverantörsrelationer

- Det ska finnas en vägledning med informationssäkerhetskrav som ska baseras på Hjo kommuns modell för informationsklassning. Vägledningen ska användas som stöd vid extern upphandling av IT-tjänster (se intranätet, IT upphandlingsmodellen)
- Det ska finnas ett dokumentationsstöd för kontroll av IT-tjänst. Syftet med vägledningen ska vara att säkerställa att IT-tjänsten kan skydda verksamheten och dess information under hela dess livscykel

Det ska finnas en vägledning med informationssäkerhetskrav som ska baseras på Hjo kommuns modell för informationsklassning. Kravkatalogen ska kunna användas som stöd vid extern upphandling av IT-tjänster såsom system och molntjänster. Det ska finnas ett dokumenterat stöd som beskriver hur en kontroll av en IT-tjänst ska genomföras. Den ska kunna användas som stöd inför användandet av en ny tjänst eller vid kontroll av en befintlig tjänst/leverantör.

Rutiner för upphandling av IT-resurser återfinns i kap D.

Rutiner för kontroll av IT-tjänst återfinns i avsnitt kap C.

Efterlevnad och granskning

Rutiner för efterlevnad och granskning av informationssäkerhet

- Efterlevnaden av informationssäkerhetspolicyn och rutinerna för informationssäkerhet ska följas upp
- Hjo kommuns informationssäkerhet ska utsättas för oberoende extern granskning

Efterlevnad av de styrande dokumenten Informationssäkerhetspolicy och detta dokument ”Rutiner för informationssäkerhet” ska följas upp. I praktiken innebär det främst att rutinerna för informationssäkerhet granskas och följs upp; att rutinerna efterlevs och att säkerhetsåtgärder införs och får avsedd verkan. I synnerhet gäller detta de särskilda säkerhetsåtgärder som gäller för information, objekt och IT-resurser med höga skyddskrav. Granskning och uppföljning av informationssäkerhet, inklusive dess styrning, kommer att utvecklas i och med det ledningssystem för informationssäkerhet (LIS) som ska införas i kommunen då en väsentlig del i ett LIS handlar om efterlevnadskontroll. Granskning av hela eller stora delar av Hjo kommuns informationssäkerhet ska göras regelbundet, genom kommunrevisionen eller av annan granskande part. Granskning av efterlevnad av informationssäkerhet bör också genomföras av extern part, exempelvis på uppdrag av kommunrevisionen. 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 IT-chef. IT-chef avgör om kommunens ledningsgrupp behöver informeras. Granskning av IT-säkerhet för IT-resurser ska ske regelbundet för att kontrollera att inga uppenbara sårbarheter exponeras och att tillräcklig säkerhetsnivå upprätthålls. Detta regleras av rutiner i Kapitel D – Informationssäkerhet i IT-miljön.

Kapitel C Verksamhetsnära informationssäkerhet

Inledning

Hjo kommun tillämpar ett linjeansvar för informationssäkerhet dvs verksamhetschef ansvarar för de system som finns inom verksamheten. Kommunens principer och modell för detta ansvar beskrivs i detta kapitel. I följande kapitel D kompletteras denna information utifrån IT-enhetens roller/ funktion.

Roller och ansvar

Här beskrivs ansvar rörande informationssäkerhet för rollerna i den verksamhetsnära förvaltningen. Motsvarande ansvar för de IT-nära rollerna återfinns i Kapitel D –informationssäkerhet i IT-miljön. Som nämnts ovan är dessa ansvar tillägg till generella ansvar enligt styrningsmodell.

Verksamhets-/ enhetschef tillika systemägare

I enlighet med Hjo kommuns informationssäkerhetspolicy är systemägaren ansvarig för systemets informationssäkerhet. Systemägarens motsvarighet i den IT-nära förvaltningen är systemägare IT (dvs IT-chef).

Systemägaren ansvarar för att Hjo kommuns informationssäkerhetspolicy och dessa rutiner efterlevs i systemet. Systemägaren ska besluta om ett systems informationssäkerhetsnivåer genom klassning, klassningen sker i enlighet med Hjo kommuns modell för informationsklassning. Systemägaren ska tilldela tillräckligt med resurser i systemets förvaltningsplaner så att informations-säkerhetsnivån kan uppnås. Verksamhets-/ enhetschef tillika systemägare kan vid behov delegera arbetsuppgifter till systemansvarig.

Systemansvarig

Systemansvarig ansvarar för att utföra informationssäkerhetsrelaterade aktiviteter på uppdrag av systemägaren. Systemägaren ansvarar för informationen i en viss informationstillgång/system dvs informationsägarskapet men kan i vissa fall delegera ansvaret tillfälligtvis till systemansvariga.

Dokumentation av informationssäkerhet

Informationssäkerhet i systemförvaltningsplaner

- Informationsrelaterade mål och åtgärder ska finnas med i ett systems förvaltningsplan
- System ska ha en systemsäkerhetsbeskrivning där systemets informationssäkerhet är dokumenterad
- Denna systemsäkerhetsbeskrivning ska gås igenom och vid behov revideras, förslagsvis årligen

Informationssäkerhet ska vara en naturlig del i förvaltningen av verksamheternas system. Säkerhetsförhållanden ska vara dokumenterade i systemsäkerhetsbeskrivningar och planerade säkerhetsåtgärder ska ingå i förvaltningsplan så att de formellt fastställs av systemägaren och ha en budget. Informationssäkerhetsmål och -åtgärder kan uppkomma eller motiveras med exempelvis resultat från riskanalyser och revisioner, erfarenheter från inträffade incidenter eller krav i dessa rutiner.

Systemsäkerhetsbeskrivning

Systemets säkerhetsförhållanden ska dokumenteras i systemsäkerhetsbeskrivningar. En systemsäkerhetsbeskrivning ska finnas för varje system. Av systemsäkerhetsbeskrivningen ska det framgå:

- Vilka informationstillgångar som hanteras i systemet och hur dessa är klassade
- Hur systemet är klassat
- Hur behörighetshantering och loggning går till

- Hur ändringshantering går till
- Användarinstruktioner med inriktning på säkerhet
- Planerade och genomförda riskanalyser och resultat från dessa
- Hur incidenthantering går till och vilka incidenter som har inträffat med referenser till incidentrapporter
- Vilken kontinuitetshantering som finns

Informationsklassning och systemklassning

Rutiner klassning av förvaltningsobjekt

- Kritiska informationstillgångar i system ska vara inventerad och klassad enligt Hjo kommuns modell för informationsklassning
- System ska klassas som helhet baserat på den klassning som är gjord av kritisk information i systemet
- Särskilda rutiner och regler för ett system ska upprättas för hantering av Hög Sekretess information, som exempelvis skyddade personuppgifter

Informationsklassning innebär att information klassas i olika nivåer utifrån dess skyddskrav. Genom att klassa information på detta sätt kan man identifiera känslig och kritisk information så att denna får tillräckligt skydd, men ibland också för att undvika att information får onödigt överskydd med höga kostnader som följd. System ska också klassas och den klassningen ska baseras på hur den ingående informationen är klassad. Klassning av information och system ska ske i enlighet med Hjo kommuns modell för informationsklassning som beskrivs i Kapitel B.

Informationsklassning ska ske utifrån rättsliga krav som lagar och föreskrifter, men även interna krav på informationens värde, känslighet och betydelse för Hjo kommuns verksamheter.

Frågor man ska ställa sig när man klassar är:

- Vilka konsekvenser blir det om informationen läcker till obehöriga (konfidentialitet)?
- Vilka konsekvenser blir det om informationen är felaktig eller inaktuell (riktighet)?
- Vilka konsekvenser blir det om (behöriga) inte får tillgång till informationen (tillgänglighet)?

När man klassar en informationstillgång enligt modellen ska den bedömas utifrån alla tre aspekter och får då en viss klassningsprofil. En viss informationstillgång kan exempelvis vara mycket kritisk när det gäller tillgänglighet och riktighet, men mindre känslig när det gäller konfidentialitet. En sådan informationstillgång kan då få klassningsprofilen 1-2-2.Klassning av ett system ska baseras på klassningen av den information som systemet hanterar. Ett system kan lägst ges den klassning som den ingående informationen har.

Exempel:

Informationsmängd	Konfidentialitet	Riktighet	Tillgänglighet
Mängd 1	0	1	1
Mängd 2	1	2	1
Mängd 3	1	1	2
Systemklassning	1	2	2

Om ett system innehåller många olika mängder information som ännu inte är klassad kan man behöva göra preliminär klassning av systemet tills all informationsklassning är gjord. Om man vet att det finns höga skyddskrav för någon informationstillgång i någon aspekt så får systemet automatiskt höga skyddskrav för denna aspekt. Vid osäkerhet är det bättre att ”överklassa” än att underklassa”.

Det viktiga är att kritisk information, dvs information med höga skyddskrav i någon av de tre

aspekterna, är identifierad och klassad därefter så att tillräckligt skydd kan skapas för systemet. Hur system klassats utgör ett underlag vid kommunikation och kravställning mot den IT-nära förvaltningen eller mot externa leverantörer. Kapitel D riktar sig mot kommunens IT-funktion och där finns särskilda säkerhetsåtgärder för system med höga skyddskrav. Klassningen av system ger också ett underlag för hur användare kan och får arbeta i system. I Kapitel A som riktar sig till samtliga medarbetare finns en mängd hanteringsregler som i vissa fall skiljer sig beroende på hur information är klassad. Särskilda rutiner och regler ska upprättas för hantering av Hög Sekretess information, som exempelvis skyddade personuppgifter. Sådana rutiner och regler ska finnas med i användarinstruktioner.

Behörighetshantering och loggning

Rutiner för behörighetshantering och loggning

- Det ska finnas dokumenterade processer och/eller rutiner för hantering av behörigheter och rättigheter till system
- Varje användare ska ha ett unikt Användar-ID
- Externa användares åtkomst bör vara tidsbegränsad samt föregås av sekretessförbindelse.
- Det ska finnas dokumenterade rutiner för logghantering i objekt
- Höga skyddskrav på konfidentialitet, riktighet eller tillgänglighet innebär också höga krav på spårbarhet. Loggning av användares aktiviteter i sådana system är obligatorisk
- Förändringar i anställningar och roller ska omedelbart rapporteras av närmaste chef till personalavdelningen så att reglering sker i personal- och lönesystem
- Uppföljning ska ske av behörighetshantering och logghantering i objekt

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.

För att skydda information mot obehörig åtkomst behöver användare ange en identitet som kan verifieras (autentiseras), vanligen med användar-ID och lösenord. Ju känsligare information som bearbetas, desto högre är kravet på skydd mot obehörig åtkomst. Grundprincipen för behörighet ska baseras på vilken information användare behöver för att kunna utföra sina arbetsuppgifter (s k need-to-know). Olika roller som använder ett system kan ha olika behov av information och ska därför ha olika typer av behörigheter eller s k åtkomstprofiler. En förutsättning för rätt behörighetstilldelning är att informationen är strukturerad och klassad så att rätt åtkomstregler kan upprättas. Inom vissa områden, som t ex vård och omsorg, behöver man ha (teknisk) behörighet till en stor mängd information. I akuta situationer måste kanske annan vårdande personal än den ordinarie ha åtkomst till patientinformation. Här behövs istället regelstyrd åtkomstkontroll, där regler säger att man inte får ta del av information som inte rör ens arbetsuppgifter. Sådan åtkomstkontroll måste kompletteras med funktioner för uppföljning, övervakning och loggning. Detta kan – och ska – påverka användarna så att dessa avhåller sig från otillåtna men tekniskt möjliga operationer i ett system. Systemägare bestämmer vilka som ska få tillgång till system och vilka behörigheter dessa ska ha. Verksamhetens art och dess krav på informationens konfidentialitet och riktighet, tillsammans med legala krav som lagar, föreskrifter och avtal, styr hur behörigheterna ska se ut. 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. Varje användare ska ha ett unikt Användar-ID, dvs. gruppidentiteter är inte tillåtna (under vissa förutsättningar kan dock detta beviljas). Det ska finnas en process eller rutiner som underhåller och förvaltar behörigheter för ett system, 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. För priviligierade användare med särskilda åtkomsträttigheter (administratörer) ska revision ske med kortare intervall. Särskild uppmärksamhet kan behöva ägnas då medarbetare med priviligierade åtkomsträttigheter slutar eller byter tjänst. Sådana processer eller rutiner måste vara kopplade till den IT-enheten så att tekniska förändringar genomförs. IT-enheten ska säkerställa den del av rutinen som rör införande, förändring samt borttagning av åtkomst i IT-resurser. I Kapitel D finns rutiner för hur åtkomstkontroll ska ske i IT-miljön. Exempelvis ska stark autentisering finnas för åtkomst till system som innehåller information med höga skyddskrav på konfidentialitet och riktighet.

Vid anställning, förändring av roll eller arbetsuppgifter samt vid upphörande av anställning ska närmaste chef omedelbart rapportera detta till personalavdelningen så att reglering sker i personal- och lönesystemet.

Processer och rutiner för behörighetshantering ska följas upp och dokumenteras.

Logghantering

För att erhålla spårbarhet och att exempelvis möjliggöra incidentutredningar samt för att upptäcka avvikelser från legala eller interna regelverk bör system övervakas och loggas avseende användaraktiviteter, avvikelser, fel och informationssäkerhetshändelser. Detta är särskilt viktigt, och obligatoriskt, om system hanterar information med höga skyddskrav eller om regelstyrd behörighetshantering används i stället för teknisk dito. Då loggning används ska det finnas processer eller rutiner för dess hantering. Sådana ska innefatta hur loggning går till, hur loggar skyddas mot manipulation och obehörig åtkomst, hur länge de sparas och hur de granskas. I de fall logginformation går att knyta till en enskild person är de att betrakta som personuppgifter och omfattas då av Dataskyddsförordningen. Detta innebär bland annat att om kontroller utförs för andra syften än det ursprungliga är lagkravet att personen ska informeras och ge sitt samtycke. Processer och rutiner för loggning ska följas upp och dokumenteras.

Ändringshantering

Rutiner för ändringshantering

- Det ska finnas dokumenterade processer eller rutiner för hantering av ändringar i system
- Vid avveckling av system ska en plan upprättas för hur information ska migreras, raderas eller slutarkiveras (i enlighet med den kommungemensamma arkiveringsplanen)

Ändringar i system ska ske på ett strukturerat sätt för att säkra systemets säkerhet, funktionalitet och användbarhet och för att minimera antalet fel orsakade av förändringen. Ändringar kan bero på exempelvis, önskemål från verksamhet/användare, fel eller brister, förändringar i legala krav eller nya versioner från systemleverantörer. Ändringar i system ska vara samordnade med IT-enheten.

I Kapitel D som riktar sig till den IT-enheten finns rutiner som rör bl.a. systemtest och hantering av testdata.

Avveckling av system ska ske på ett strukturerat sätt och i samråd med Kansliet så att information hanteras i enlighet med den kommungemensamma arkiveringsplanen. Större förändringar i eller omkring ett system ska föregås av en riskanalys.

Användarinstruktioner

Rutiner för användarinstruktioner

- Informationssäkerhetsregler ska finnas med i användarinstruktioner
- Det ska finnas särskilda instruktioner för hantering av konfidentiell information som t ex skyddade personuppgifter

Systemägare ansvarar för att det finns användarinstruktioner för samtliga användare till ett system. Användare ska utbildas enligt instruktionerna och kontroll ska göras att instruktionerna efterlevs. Användarinstruktionerna ska omfatta följande delar inom informationssäkerhet:

- Regler kring inloggning och lösenordshantering
- Behörigheter
- Särskilda instruktioner för hur konfidentiell information får hanteras, t ex känsliga eller skyddade personuppgifter
- Information om vad som loggas och konsekvenser av att bryta mot användarinstruktioner, t ex att ta del av eller sprida konfidentiell information
- Incidentrapportering – användare ska vara vaksamma på brister och incidenter i systemet och veta hur man ska rapportera dessa
- Eventuell sekretessförbindelse

Användare är naturligtvis även skyldiga att följa rutinerna i Kapitel A.

Riskanalys

Rutiner för riskanalyser

- Riskanalyser ska genomföras i samband med större förändringar i eller omkring system
- Riskanalysresultat ska dokumenteras. Akuta risker ska tas om hand skyndsamt och återstående åtgärder ska tas med i förvaltningsplaner
- Ett riskhanteringsbeslut ska fattas för varje allvarlig risk som identifieras under riskbedömning. En åtgärdsplan kan vara ett sådan riskhanteringsbeslut

Risker är tänkbara oönskade händelser som kan inträffa och som kan ha en negativ påverkan på mål. Antingen på mål med själva systemet eller på verksamheters mål. En risk är en kombination av hur sannolikt det är att en händelse inträffar och vilken konsekvens händelsen innebär. Vid större förändringar, t ex större systemuppdateringar, nyutveckling, nya användargrupper eller extern åtkomst, liksom när en ändring påverkar andra system som inte förvaltas inom samma objekt, ska en riskanalys genomföras där Hjo kommuns grundmetod för riskanalys ska användas. Det kan också vara förändringar utanför själva systemet eller dess kontroll som motiverar en riskanalys, exempelvis ägarbyte av en systemleverantör eller en omorganisation som berör den verksamhet som systemet stödjer. Riskanalysens resultat ska dokumenteras. En riskanalys kan leda till åtgärdsbehov som behöver genomföras omedelbart eller på lite längre sikt och kan då tas med i kommande förvaltningsplan.

Incidenthantering

Rutiner för incidenthantering

- Det ska finnas rutiner för hur användare ska rapportera incidenter
- Akuta incidenter ska åtgärdas skyndsamt
- Allvarliga incidenter ska utredas och dokumenteras enligt gällande rutin
- Avbrottsplaner ska upprättas som innehåller ansvarsförhållanden, kontaktpersoner och eskaleringsvägar

- Samtliga incidenter som rör systemet ska dokumenteras och sammanställas. Kvarstående åtgärdsbehov ska tas om hand i förvaltningsplaner
- Personuppgiftsincidenter kopplade till system ska anmälas enligt särskild rutin

Informationssäkerhetsrelaterade incidenter är oönskade händelser som kan, eller skulle kunnat, leda till brister i konfidentialitet, riktighet eller tillgänglighet hos information. Systemägare ansvarar för att incidenter relaterade till system upptäcks, samlas in, hanteras, sammanställs och dokumenteras.

Incidenter kan delas in i mindre incidenter och allvarliga incidenter (major incidents). Mindre incidenter är t ex mindre tekniska fel i system eller att enstaka användare inte följer användarinstruktioner. I systemets användarinstruktioner ska det finnas rutiner för hur användare ska rapportera mindre incidenter. Incidentrapporter ska mottas och lämpliga åtgärder ska vidtas.

Allvarliga incidenter är större störningar i ett system som t ex ett längre avbrott (några timmar eller mer), dataintrång eller infektion av skadlig kod. En allvarlig incident kräver en utredning där dokumentation ska göras enligt gällande mall för allvarliga IT-relaterade incidenter. Utredningen ska drivas av IT-chef i samverkan med relevanta aktörer, inte minst med Skövdes IT-avdelning som samverkanspart. Om personuppgifter behandlas ska en anmälan om personuppgiftsincident göras. Personuppgiftsincidenten utreds separat men resultatet från IT-enhetens utredning kan användas som underlag för bedömning av personuppgiftsincidenten, en samordning mellan person-uppgiftssamordnare och IT-chef kan därför vara lämpligt. Systemägare/verksamhets-/enhetschef ska upprätta avbrottsplaner att använda vid större avbrott och som ska innehålla ansvarsförhållanden, kontaktpersoner, eskaleringsvägar till interna och externa aktörer. Här ska samverkan ske med den IT-enheten.

Flera fall av mindre incidenter av likadan art kan tillsammans utmynna i eller utgöra en allvarlig incident. Ett antal störningar i systemet av samma typ som var för sig betraktas som mindre incidenter kan tillsammans innebära en allvarlig incident. Både mindre och allvarliga incidenter kan vara av akut art och behöva åtgärdas skyndsamt. IT-chefen ska årligen sammanställa samtliga incidenter som varit kopplade till system och som har haft eller kunde ha haft påverkan för verksamhetens informationssäkerhet. Sammanställningen ska redovisas till systemägare för verksamhetssystemet, dokumentet är en viktig indata till ledningens genomgång av informations-säkerhet. Kvarstående åtgärdsbehov som inträffade incidenter medfört ska tas om hand i förvaltningsplaner.

Kontinuitetshantering

Rutiner för kontinuitetshantering

- Reservplaner och manuella rutiner ska finnas för kritiska objekt med höga skyddskrav gällande tillgänglighet
- Nyckelpersonsberoende ska undvikas och åtgärdas

Krav på kontinuitet av driften av system sker i stora delar genom klassning. Höga skyddskrav för tillgänglighet innebär högre krav på säkerhetskopiering och redundans. Avbrott kan dock ändå alltid ske oavsett vilka förebyggande skyddsåtgärder som finns. Beroendet av funktionalitet av system kan ibland vara så högt att systemen helt enkelt inte får ligga nere. I dessa fall måste verksamheten ha planer och rutiner för att kunna fullfölja sitt åtagande även vid teknikavbrott. Nyckelpersons-beroende ska undvikas och i den mån det framkommer att organisationen är beroende av nyckelpersonal ska nyckelpersonberoendet åtgärdas t ex genom utbildning av ersättare. Nyckelpersonsberoende kan också minskas genom att använda vedertagen standard och standardprodukter.

Kontroll av IT-tjänst

Rutiner för kontroll av IT-tjänst

- Innan en verksamhetsansvarig börjar använda en IT-tjänst ska den kontrollera (enligt vägledningen för kontroll av IT-tjänst) att tjänsten kan leverera rätt skydd för verksamhetens information
- Innan en verksamhetsansvarig börjar använda en IT-tjänst ska den ta beslut kring de risker som ett sådant användande kan ge upphov till
- Endast information som är klassad (informationsklassning) får användas i externa IT-tjänster och molntjänster
- Känslig Sekretess (Gul) och Hög Sekretess (Röd) får endast lagras i en IT-tjänst som är tillräckligt kontrollerad, risken acceptabel och att lagringen av information inte bryter mot några författningar
- IT-tjänster som lagrar Känslig Sekretess (Gul) och Hög Sekretess (Röd) information ska kontrolleras minst en gång om året

Verksamhetschef är ansvarig för informationssäkerheten inom sitt verksamhetsområde, det innebär även att säkerställa att dess processer, verktyg, personal och resurser har rätt skyddsnivå.

Korrekt informationssäkerhet ska säkerställas under hela livscykeln och innebär att verksamhetchef behöver försäkra sig om att rätt skyddsnivå är uppnådd och tydligt acceptera eventuella risker. Att avgöra rätt skyddsnivå innebär bland annat att genomföra verksamhets- och juridiska analyser genom informationsklassningar. Förutom att kontrollera en IT-tjänst innan användning är det lämpligt att genomföra kontroller med jämna mellanrum i den frekvens som verksamheten finner lämpligt.

Kapitel D Informationssäkerhet i IT-miljön

Inledning

Detta kapitel innehåller rutiner rörande säkerhet Hjo kommuns IT-miljö. Rutinerna vänder sig därför främst till Hjo kommuns IT-enheten samt Skövde kommuns IT-avdelning i rollen som samverkanspart/ driftsleverantör. Rutinerna riktar sig också till externa parter som arbetar på uppdrag åt Hjo kommun, exempelvis inhyrda konsulter. Informationssäkerhet i IT-miljön kan även benämnas IT-teknisk säkerhet och innefattar säkerhet i olika slag av IT-resurser som system, applikationer, 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 som till största delar innehåller säkerhet i IT-miljöer:

Avsnitt i Kapitel D	Relaterade avsnitt 27002
Hantering av tillgångar	Kap 8
Styrning av åtkomst	Kap 9
Kryptering	Kap 10
Fysisk och miljörelaterad säkerhet	Kap 11
Driftsäkerhet	Kap 12
Kommunikationssäkerhet	Kap 13
Anskaffning och utveckling av IT system	Kap 14
Incidenthantering	Kap 16
Kontinuitetshantering	Kap 17
Granskning och kontroll	Kap 18

Standarden innehåller mer vägledning och information än vad som finns i dessa rutiner, och standarden kan därför användas som ett stödjande dokument för att efterleva rutinerna. Inom vissa områden i IT-miljön behöver mer detaljerade instruktioner tas fram som kompletterar eller konkretiserar dessa rutiner. Även för detta ändamål kan denna eller andra standarder liksom andra vägledningar, från t ex MSB, vara till stöd. En central del i kommunens informations-säkerhetsarbete är informationsklassning. Information kan ha normala eller höga skyddskrav avseende konfidentialitet, riktighet och tillgänglighet i enlighet med Hjo kommuns klassningsmodell. IT-resurser som hanterar information ska ges ett skydd i enlighet med dessa skyddskrav.

Roller och ansvar

Ansvaret för informationssäkerhet ligger ytterst på IT-chefen. Därigenom är IT-chefen ytterst ansvarig för att säkerheten i IT-miljö som tjänster, processer, system, infrastruktur, verktyg etc. är tillräcklig och uppfyller verksamheters krav, legala krav samt informationssäkerhetspolicyn och dessa rutiner för informationssäkerhet.

IT-säkerhetsansvarig

I IT-chefsansvaret ingår rollen IT-säkerhetsansvarig. Rollen samordnar arbetet med säkerheten i Hjo kommuns IT-miljö i nära samverkan med Skövde kommuns IT-avdelning, och är stödjande vid kravställning på externa aktörer. Ansvaret för säkerheten i IT-resurser ligger inte på den IT-

säkerhetsansvarige, utan dennes roll är att kravställa, stödja och kontrollera arbetet med att nå och upprätthålla rätt nivåer av säkerhet i dessa.

För den IT-säkerhetsansvarige innebär detta i huvudsak att:

- utforma och förvalta rutiner och instruktioner för IT-säkerhet
- stödja verksamheter, förvaltningsobjekt och projekt i IT-säkerhetsfrågor
- följa upp och granska efterlevnaden av rutiner och instruktioner för IT-säkerhet
- stödja och bevaka framtagning och genomförande av handlingsplaner för att åtgärda brister som konstaterats i samband med säkerhetsgranskningar eller riskanalyser
- bistå vid utredning av misstänkta och inträffade säkerhetsincidenter
- stödja verksamheter vid extern kravställning rörande IT-säkerhet och uppföljning av externa leverantörers säkerhetsåtaganden
- leda eller delta i verksamheters riskanalyser rörande IT-relaterade risker
- verka för höjande av säkerhetsmedvetande inom IT
- ta fram statusrapporter för kommunens IT-säkerhet, och besvara revisionsrapporter
- utifrån behovsanalyser kravställa på leverantörer

I rollen ingår även att omvärldsbevaka, nätverka och samverka externt inom området med exempelvis MSB, cert.se, SIG Security, SKL och andra kommuner.

Roller i den IT-nära förvaltningen

Systemägare IT tillika IT-chef

Systemägare IT ansvarar för att IT-säkerheten i IT-systemen överensstämmer med verksamhetens krav så att rätt säkerhetsnivå upprätthålls och att aktuella IT-system ges ett skydd som motiveras av klassningen av system. Systemägare IT:s motsvarighet i den verksamhetsnära förvaltningen är verksamhets-/ enhetschef (systemägare). Systemägare IT ansvarar för att Hjo kommuns informationssäkerhetspolicy och dessa rutiner efterlevs.

Systemtekniker IT

Systemtekniker IT ansvarar för att utföra IT-säkerhetsrelaterade aktiviteter på uppdrag av systemägare IT.

Incident manager (finns detta i Skövde?)

En Incident Manager bevakar och analyserar incidentprocessen samt ansvarar för att rutiner för eskalering, larm och informationsspridning samt andra processer följs.

Hantering av tillgångar

Rutiner för hantering av tillgångar

- Samtliga IT-resurser ska identifieras
- Samtliga IT-komponenter som elektroniskt lagrar och bearbetar information och där information ägs av kommunal myndighet ska förtecknas. Rutiner ska finnas för att hålla förteckningen aktuell och den ska skyddas från åtkomst eller förändring av obehörig
- IT-komponenter ska klassas baserat på klassningen av den information som hanteras i IT komponenten och/eller baserat på klassningen av andra objekt som IT-komponenten stödjer eller påverkar
- Skyddsåtgärder i en IT-komponent ska motsvara dess klassning så att rätt nivå av IT-säkerhet upprätthålls under IT-komponentens hela livscykel, såväl vid införande, under drift som efter avveckling
- Informationssäkerhetskrav som gäller användandet av IT-komponenter ska förmedlas till användare i form av användningsinstruktioner.

Identifiering av IT-resurser och tilldelning av ägare

Samtliga IT-resurser ska vara identifierade och tilldelade en ägare. En förteckning över alla IT-resurser ska upprättas och underhållas. Förvaltningsobjekt som omfattas av förvaltnings-organisationen, exempelvis verksamhetssystem, har naturliga ägare inom IT i form av systemägare.

Klassning av IT-resurser

IT-komponenter ska klassas i enlighet med Hjo kommuns 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-komponenter i form av infrastruktur, stödsystem m.m. ska ges minst motsvarande klassning. Ibland kan sådana underliggande IT-komponenter 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-komponenter och till klassade verksamhetssystem, får man klassa IT-komponenten utifrån en bedömning enligt konsekvensbeskrivningarna i klassningsmodellen. Eftersom långt ifrån all information och alla IT-komponenter är klassade inom kommunen, kan preliminära klassningar behöva göras för IT-komponenter. Vid osäkra fall är det viktigt att hellre ”överklassa” än ”underklassa”. Beroende på hur IT-komponenter är klassade ska olika säkerhetsåtgärder införas för att uppnå ett tillräckligt bra skydd. Bland annat ska dessa rutiner följas som riktar sig mot IT-miljön och som i vissa fall har särskilda krav för IT-komponenter som hanterar information med höga skyddskrav enligt en eller flera aspekter av konfidentialitet, riktighet och tillgänglighet. Ägare till IT-komponenter ansvarar

för att säkerhetsnivån är tillräcklig över IT-komponentens hela livscykel, såväl vid införande, under drift som under avveckling.

Användningsinstruktioner

Det ska finnas regler och instruktioner till hur IT-komponenter får användas. Dessa ska

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

Styrning av åtkomst

Rutiner för identifiering och autentisering

- 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 namnuppgift i folkbokföringen
- Vid åtkomst till information med höga skyddskrav avseende konfidentialitet eller riktighet ska stark autentisering användas
- Stark autentisering är krav vid fjärråtkomst till Hjo kommuns IT-miljö
- Fjärråtkomst för inloggning med administrativa (priviligierade) konton till IT-resurs med höga skyddskrav avseende konfidentialitet eller riktighet skall vara strikt styrt
- 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-komponenten 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
- 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

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 uppgifter. 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 behörighets-kontrollsystem (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

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 Hjo 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.

Reglering av åtkomsträttigheter

Rutiner för reglering av åtkomsträttigheter

- Det ska finnas beslutade och dokumenterade regler och rutiner för behörighetshantering, dvs. BKS, i IT-resurser
- IT-resurser ska ha åtkomsträttigheter som motsvarar hur de är klassade
- Användaridentiteter och vilka individer dessa tillhör ska registreras i en gemensam AD-katalog och rutin ska finnas för att hålla denna katalog 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
- Behörigheter till IT-resurser ska vara aktuella och riktiga.
- Åtkomst som inte längre behövs eller behov av ny åtkomst ska regleras snarast, för IT-resurser inom en arbetsdag efter att behov upphör eller uppstår. Det ska finnas rutiner kopplade till personalfunktionen 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. IT systemägare beslutar om tilldelning av priviligierad åtkomsträtt. Granskning av administrativa rättigheter ska ske löpande med täta intervall
- Gruppidentiteter är inte tillåtna. Eventuella undantag ska godkännas av systemägare verksamhet och IT-chef 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, konsultförbindelse
- Prövning av den enskilde ska ske och den anställde ska skriva på en sekretessförbindelse som används för att påminna om tystnadsplikten innan åtkomst tilldelas till IT-resurs som innehåller information med höga skyddskrav avseende konfidentialitet
- Närmaste chef fattar beslut om behörighet till informationssystem och -tjänster, denne är

också ansvarig för att beställa inaktivering eller avslut av behörigheter

Åtkomst till IT-resurser 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 systemägare/verksamhetschef i verksamheten som beslutar vilka som ska få tillgång till systemet och vilka behörigheter dessa ska ha, samt hur systemet är klassat. Systemägare IT ansvarar för att upprätta ett BKS som motsvarar dessa krav.

Det ska finnas beslutade och dokumenterade regler och rutiner för behörighetshantering, dvs. BKS, i IT-resurser. 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 personalenheten 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 den anställde ska skriva på en sekretessförbindelse som används för att påminna om tystnadsplikten. 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. Regelbunden uppföljning och revision av samtliga åtkomsträttigheter ska ske kontinuerligt. För priviligierade användare med särskilda åtkomsträttigheter (administratörer) ska 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.

Säkerhetsloggning

Rutiner för säkerhetsloggning

- 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 informations-säkerhetshändelser, ska skapas, bevaras en bestämd tid och granskas regelbundet. För loggar som innehåller systemadministratörers aktiviteter gäller att de ska granskas av loggadministratör som inte är samma person som systemadministratören

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 IT-resurser övervakas och loggas avseende användaraktiviteter, avvikelser, fel och informations-säkerhetshändelser. 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 Dataskyddsförordningen. 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 en ny rättslig grund för person-uppgiftsbehandlingen måste hittas, t ex samtycke, innan den får ske.

Kryptering

Rutiner för kryptering

- Krypteringslösningar ska baseras på etablerade standarder och införande ska godkännas av IT-chef
- Nyckelhantering ska säkerställas för att tillgodose de krav som finns för IT-resurs avseende
    - Revokering av nycklar
    - Validering av nycklars giltighet och autenticitet
    - Återställning av nycklar
- Krypteringsnycklar är konfidentiell information och ska skyddas därefter

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 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 objektägare IT i samråd med verksamhetsansvarig och IT-chef. Införande av krypteringslösningar ska godkännas av IT-chef. Viktigt att tänka på är att ibland kan krypteringslösningar medföra nya risker relaterade till nyckelhantering.

Fysisk och miljörelaterad säkerhet

Rutiner för fysisk och miljörelaterad säkerhet

- 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. Roller med ansvar 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 i möjligaste mån 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 med IT-resurser för att undvika säkerhetsrisker
- 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.
- IT-resurser ska skyddas från elavbrott och andra störningar som orsakas av fel i tekniska försörjningssystem
- Synliga 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
- Underhåll och reparation ska utföras på sådant sätt att information eller IT-resurs inte riskerar att röjas eller skadas. Om utomstående ska utföra underhåll på IT-resurs med höga skyddskrav ska sekretessavtal tecknas. Vid känslig information ska informationen döljas, flyttas eller raderas från utrustningen
- Avveckling eller skrotning av IT-resurser och datamedia ska, efter att information som ska bevaras ha förts över till kommunarkivet, 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

Fysisk och miljörelaterad säkerhet avser att förhindra otillåten fysisk åtkomst till, skador på och störningar i IT-resurser. 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 skyddsvärda IT-resurserna är.

Säkra utrymmen för IT-resurser

Säkra utrymmen med särskilda säkerhetskrav är exempelvis rum som används för servrar, switchar och annan kommunikationsutrustning samt e-arkiv. För IT-funktioner är det främst datorhallar och serverrum 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. Roller med ansvar 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 etcetera. 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 IT-resurser med höga skyddskrav ska bevakas och fysisk närvaro ska loggas (till exempel tillträdes- eller videoövervakningsloggar).

Godsmottagning och lastning

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 vid leveranstillfället och eventuella avvikelser från förväntad leverans ska kvitteras av leverantören.

Underhåll, reparation och avveckling

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 IT-resursen eller tillträde till sådana säkra utrymmen där IT-resurser

finns placerade och detta kräver därför särskild uppmärksamhet. Om underhåll och reparation ska utföras av utomstående på IT-resurs med höga skyddskrav avseende konfidentialitet ska vederbörande alltid underteckna sekretessavtal. Det kan ibland vara nödvändigt att vidta särskilda åtgärder, till exempel att känslig information flyttas, raderas eller krypteras innan någon utomstående hanterar utrustningen. Detsamma gäller avveckling av IT-resurser 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 till exempel behöva skrivas över eller destrueras på ett säkert sätt innan den sänds till skrotning eller återanvändning. Observera att datamedia kan finnas i olika typer av IT utrustning till exempel skrivare.

Skydd av utrustning

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, till exempel där många externa personer frekvent vistas och i publika lokaler. Där krävs stöldskydd (till exempel fastlåsning) och märkning. Speciellt utsatt är också mobil utrustning där risken för förlust, stöld och skada är högre. Användning ska ske i enlighet med de instruktioner som gäller vid distansarbete och mobil utrustning där användare till exempel ska säkerställa att utrustning antingen övervakas eller låses in för att minska risken för stöld.

Elförsörjning

Säker elförsörjning (till exempel avbrottsfri kraft genom UPS och reservkraft) ska finnas så att IT-resurser skyddas från elavbrott och andra störningar som orsakas av fel i tekniska försörjnings-system.

Driftsäkerhet

Regler för driftrutiner

- Det ska finnas formella, beslutade och dokumenterade driftsrutiner för väsentliga processer och objekt. Dessa ska göras tillgängliga för alla användare som behöver dem
- Ändringar i IT-resurser ska följa fastställd process som säkerställer att ändringarna är riskbedömda, planerade, kommunicerade, testade och godkända (liknande ITIL Change Management)
- Utvecklings-, test- och driftmiljöer ska vara separerade för att minska risken för obehörig åtkomst eller ändringar i driftmiljön

Dokumenterade driftsrutiner ska finnas och göras tillgängliga för alla användare som behöver dem.

Driftsrutiner ska vara formella och beslutade dokument. Förändringar i IT-resurser ska styras enligt fastställd ändringshanteringsprocess. 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.

Skydd mot skadlig kod

Rutiner för skydd mot skadlig kod

- 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
- IT-resurser som stöder objekt 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 IT-resurser 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)

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-resurser 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, Skadlig kod). Kommunens IT-resurser ska skyddas från skadlig kod genom att antivirusprogramvara installeras på klienter och servrar. Skyddet ska regelbundet uppdateras. 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

IT-resurser 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 IT-resurser (se avsnitt Incidenthantering). 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).

Säkerhetskopiering

Rutiner för säkerhetskopiering

- För IT-resurser med höga skyddskrav avseende tillgänglighet ska redundans finnas i delkomponenter, system, lagring och nätverk samt säkerställd infrastruktur för IT-drift
- Tillgänglighet ska övervakas för att säkerställa att viktiga kvalitetsmått uppfylls
- Baserat på objekts klassning av riktighet och tillgänglighet ska krav definieras för säkerhetskopiering av information
- Det ska finnas en process för återlagring från säkerhetskopia, processen ska vara testad och dokumenterad
- 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

Säkerhetskopiering av information, program och speglingar av system är en viktig del av drifts-säkerheten. Detta ger möjlighet att återställa en IT-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 IT-resurser 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 till exempel 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 Fysisk och miljörelaterad säkerhet). Säkerhetskopior ska testas regelbundet för att säkerställa att återlagring fungerar som avsett.

Loggning och övervakning

Rutiner för loggning och (system)övervakning

- 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 systemägarens krav
- För att säkerställa all typ av loggning av händelser ska systemklockorna i alla relevanta IT-resurser synkroniseras mot en betrodd referenskälla för korrekt tid
- Loggningsverktyg och logginformation har höga skyddskrav och ska skyddas mot manipulation och obehörig åtkomst

Övervakning och loggning gör det möjligt att upptäcka händelser i IT-resurser. 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 informations-säkerhetshändelser 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. Krav på loggar och övervakningssystem kan variera beroende på IT-resursens art och användningsområde. Det är IT-resursens klassning och systemägarens 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.

Hantering av tekniska sårbarheter

Rutiner för hantering av tekniska sårbarheter

- Det ska finnas rutiner för att få information om, upptäcka, analysera och åtgärda tekniska sårbarheter i IT-resurser. Uppdateringar och säkerhetspatchningar ska göras regelbundet på IT-resurser
- I de fall säkerhetspatchning inte är praktiskt möjlig, ska information om tekniska

sårbarheter i sådana IT-resurser inhämtas och analyseras och lämpliga åtgärder vidtas för att hantera den tillhörande risken
- Säkerhetsgranskning av IT-resurser ska ske regelbundet och för verksamhetskritiska resurser minst årligen 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 och appar en användare kan installera och på vilket sätt

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. Okontrollerad installation av program kan medföra sårbarheter och incidenter, som exempelvis obehörig åtkomst till information, förlust av riktighet eller överträdelse av immateriella rättigheter. Regler för programinstallationer som utförs av användare ska upprättas och införas som definierar vilka typer av program en användare kan installera och på vilket sätt.

Kommunikationssäkerhet

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

Nätverkssäkerhet

Rutiner för nätverkssäkerhet

- 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 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
- Brandväggar ska konfigureras i enlighet med zero-trust modell.
- Kommunikationstjänster mellan Hjo kommun och externa nätverk ska dokumenteras och godkännas av systemägare IT innan inkoppling får ske

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 objekt, 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 till exempel 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.

Informationsöverföring

Rutiner för informationsöverföring

- Kommunikation med höga skyddskrav avseende konfidentialitet och riktighet ska alltid krypteras och kommunicerande parter ska identifieras på ett säkert sätt
- 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 Hjo kommun och externa parter ska regleras genom avtal
- Kommunikation med e-post till andra organisationer skyddas i samtliga e-postsystem genom att konfigurera och aktivera standardiserade säkerhetsfunktioner

Information som hanteras genom elektronisk meddelandehantering ska ges lämpligt skydd. Om meddelande 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 Hjo 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.

Anskaffning och utveckling av IT-resurser

Korrekt informationssäkerhet för IT-resurser ska säkerställas över hela livscykeln och börjar vid anskaffning eller utveckling.

Säkerhetskrav på IT-resurser

Rutiner för säkerhetskrav på IT-resurser

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

Krav som rör informationssäkerhet ska redan från början inkluderas i kraven för nya IT-resurser likväl som i krav för förbättringar av befintliga. Det gäller oavsett om IT-resursen upphandlas externt, utvecklas internt eller en kombination av båda (till exempel anpassning av ett inköpt standardsystem). Informationssäkerhetskraven ska spegla den klassning som tilldelats IT-resursen och

som baseras på till exempel 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. Systemägare IT 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 IT-resurser 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.

Säkerhetskrav vid upphandling av IT-stöd

Rutiner för säkerhetskrav vid upphandling av IT-stöd

- 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 på begäran kunna 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 Hjo 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 Upphandlingsenheten i Skövde
- För att säkerställa tillgänglighet till källkod samt underhåll och utveckling i händelse av oväntade förändringar hos IT-leverantör eller dess underleverantörer ska för verksamhetskritiska system och applikationer så kallad källkodsdeposition användas, där minst ett exemplar av källkoden lämnas i förvar hos tredje part.
- Avtal med IT-leverantör ska innefatta:
    - Att leverantören innan leverans till Hjo kommun genomför säkerhetstestning av system och ingående komponenter.
    - Att testet 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

Vid upphandling av IT-stöd gäller ovanstående rutiner för säkerhetskrav på IT-resurser. 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 objekt, 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 eller om leverantör på annat sätt kommer få åtkomst till information tillkommer krav som kan innefatta:

- Fördjupade krav på leverantörens interna IT-miljö och informationssäkerhet (till exempel 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. Upphandling av IT-stöd ska alltid följa IT-upphandlingsmodellen och göras i samverkan med Upphandlingsenheten i Skövde.

Säkerhet vid systemutveckling

Rutiner för säkerhetskrav vid systemutveckling

- Processer, rutiner och regler ska finnas som reglerar att informationssäkerhet finns med under hela utvecklingscykeln av IT-resurser
- Systemförändringar inom utvecklingscykeln ska styras genom ändringshanteringsprocess, jmfr Change managementprocessen
- 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

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. Systemförändringar inom utvecklingscykeln ska styras genom användning av Change management-processen. 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. Om ingen etablerad modell används av leverantören krävs en betydligt mer ingående analys för att säkerställa en säker utvecklingsprocess.

Säkerhetskrav vid test

Rutiner för säkerhetskrav vid test

- Säkerhetsfunktionalitet ska testas vid utveckling och testning ska göras gentemot de ställda säkerhetskraven och i enlighet med rutiner 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:
    - Testdata ska alltid anonymiseras från personuppgifter
    - Rutiner för styrning av åtkomst som tillämpas för produktionssystem ska också gälla vid test av sådana system
    - Behörighet ska godkännas av objektägare IT varje gång produktionsdata kopieras till ett testsystem
    - Produktionsdata ska omgående raderas från testsystem efter avslutad test
    - 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
- Driftsättning ska ske enligt fastställd process för ändringshantering avseende berört objekt (jmfr Change management-process)

Säkerhetsfunktionalitet ska testas vid utveckling och testning ska göras gentemot de ställda säkerhetskraven och i enlighet med rutiner för säker utveckling. Vid test kan man dra nytta av automatiserade verktyg, till exempel 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 så långt som möjligt 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.

Driftsättning ska ske enligt ändringshanteringsprocess, jmfr Change management-process.

Incidenthantering

Rutiner för incidenthantering

- 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 korrektiva 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 systemägare ansvarar för att ta fram i samverkan med IT
- 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

Med informationssäkerhetsincident avses en händelse som har eller skulle kunnat ha försämrat konfidentialitet, riktighet eller tillgänglighet hos information. Alla medarbetare inom Hjo kommun är skyldiga att rapportera incidenter (se Kapitel A). Detta innefattar självklart även medarbetare på IT samt 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 IT support. 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.

För IT inspireras hantering av incidenter av ITIL-processen ”Incident Management”. Denna process innefattar fler typer av incidenter än vad som kan definieras som informationssäkerhetsincident enligt ovan, men incidenthanteringsprocessen måste självklart omfatta och hantera informationssäkerhetsincidenter. Dessa kan 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 korrektiva 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.
- Lessons learned

IT ska i rollen som ”incident manager” leda hanteringen av IT-incidenter i samverkan med berörda ägare av system. Vid incidenter relaterade till förvaltningsobjekt ska IT samverka

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 objektägare ansvarar för att ta fram i samverkan med incident manager. 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.

Krisorganisation och krisplan

Rutiner för krisorganisation och krisplan

- Det ska på IT finnas en krisorganisation för allvarliga incidenter och kriser, som tydligt beskriver roller och ansvar
- Det ska finnas en krisplan på IT som ska aktiveras vid händelse av en allvarlig incident eller kris. Krisplanen ska bland annat innehålla krisorganisation, kontaktpersoner och operativa steg att vidta under en allvarlig störning eller kris
- Krisplanen ska testas och övas minst en gång per år. Identifierade brister och svagheter ska åtgärdas i syfte att ständigt förbättra krisplanen för IT. Övning kan ske genom s.k table-top övning eller scenarioövning

En krisplan ska finnas som ska aktiveras vid händelse av allvarliga incidenter eller kriser (sk major incidents) i IT-miljön. Krisplanen ska ha en ansvarig förvaltare och innehålla bland annat kris-organisation, kontaktpersoner och operativa steg att vidta under en allvarlig störning eller kris.

Kontinuitetshantering

Rutiner för kontinuitetshantering

- Det ska finnas avbrottsplaner för samtliga kritiska IT-resurser 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

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 till exempel personal, lokaler och verktyg. IT-resurser 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 objekt med höga skyddskrav avseende tillgänglighet måste

finnas en beredskap för hur man hanterar avbrott – sk avbrottsplaner. Systemägare IT ansvarar för att IT mässiga avbrottsplaner finns på plats för att snabbast möjligt få igång normal IT-funktionalitet. Planerna motsvarar de krav som finns för objekt.

Verksamheten ansvarar för ej IT-mässig reservplan för att upprätthålla verksamhet. Avbrottsplaner ska vara relaterade till incidenthanteringen och den övergripande krisplan som ska finnas på IT. En viktig säkerhetsåtgärd för att skapa och bibehålla hög tillgänglighet är säkerhetskopiering. Målsättningen är att kontinuitetshantering ska utvecklas i hela Hjo kommun och på sikt ingå i ett ledningssystem för informationssäkerhet.

Granskning och kontroll

Rutiner för granskning och kontroll

- Kritiska delar i IT-miljön som stödjer objekt med höga skyddskrav ska regelbundet övervakas och granskas för att sårbarheter och brister ska upptäckas
- Vid osäkerhet gällande säkerhetsförhållanden skall de IT-säkerhetsmässiga förutsättningarna ses över och lyftas till systemförvaltningen
- Sårbarheter och brister som upptäcks vid granskningar ska tas upp för åtgärdande i genomförandeplaner, till exempel förvaltningsplaner. Akuta sårbarheter och brister ska åtgärdas omedelbart
- Rapportering av större sårbarheter och brister ska ske till IT-chef. IT-chef avgör om kommunens ledningsgrupp behövs informeras
- 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 objektägare
    - Omfattningen av tekniska aktiviteter för granskning eller revision ska beskrivas för- och godkännas av IT-resursens ägare.
    - 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

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 till exempel 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, till exempel förvaltningsplaner. Akuta sårbarheter och brister ska åtgärdas omedelbart. Rapportering av större sårbarheter och brister ska ske till IT-chef och i förekommande fall till kommunens ledningsgrupp. Revision av hela eller delar av IT-miljön ska göras minst vartannat år. Revision eller mätning av Hjo kommuns informationssäkerhet i stort kan även omfatta IT-miljön.