

Riktlinjer informationssäkerhet

Norsjö kommun

Dokumenttyp	Dokumentägare	Beslutsinstans	Giltig till
Riktlinje	Kanslienheten	Kommunfullmäktige	Tillsvidare
Upprättad av	Fastställd/uppriättad	Reviderad av	Senast reviderad
Ina Jeuthe	2023-03-27	Ina Jeuthe	2024-11-07
Dokumentet gäller för Samtliga verksamheter			Diarienummer KS-24/01307



Innehållsförteckning

Inledning.....	6
Riktlinjernas omfattning.....	6
Dispenser och undantag.....	6
Struktur och läsanvisningar.....	7
Introduktion till informationssäkerhet.....	8
Termer och definitioner.....	9
Kapitel A: Informationssäkerhet för medarbetare.....	12
Inledning.....	14
A1 Övergripande regler.....	14
Medarbetares ansvar för informationssäkerhet.....	15
Skyldighet att rapportera incidenter och brister.....	16
Informationsklasser.....	17
Personuppgifter.....	19
Allmänna handlingar och sekretess.....	20
A 2 Lösenord.....	21
A3 E-post.....	23
A 4 Chatt/direktmeddelanden.....	25
A5 Lagring och säkerhetskopiering.....	25
Lagring på mobila enheter, smarta telefoner och surfplattor.....	28
A6 Mobila enheter (t ex bärbar dator, smarta telefoner, surfplattor).....	28
Särskilda regler för smarta telefoner och surfplattor.....	30
A7 Skadlig kod.....	31
Spridning av skadlig kod.....	32
A8 Internet och sociala media.....	32
A9 Spårbarhet och loggning.....	34
Rutin vid fördjupad granskning.....	35
Gallring av loggar från granskning.....	35
Pornografi.....	36
Anonymitetsservrar.....	36
Illegal fildelning.....	36
Rutin för loggning.....	36
Individuell loggning.....	37
Granskning av loggar.....	37

A10 Säkert beteende	37
Kapitel B Styrning av informationssäkerhet.....	40
Inledning.....	42
B1 Roller och ansvar	42
Grundprincip.....	42
Kommunfullmäktiges ansvar	42
Kommunstyrelsens ansvar.....	42
Ansvar inom varje utskott och dess verksamheter.....	43
Medarbetares ansvar	43
Personuppgiftsansvar	43
Arkivmyndigheten.....	44
Systemägares ansvar	44
Ansvar i projekt	44
IT-enhetens ansvar	44
IT-säkerhetsansvarig.....	45
CISO.....	45
Beredskap/räddningstjänst.....	45
Digitaliseringsgruppen - Informationsforum	45
Dataskyddsbud	46
Kommunens revisorer	47
B2 Dokumentstruktur	47
B3 Informationsklassning.....	49
Vad ska klassificeras?.....	52
Användningsområden och målgrupper	52
B4 Ledningssystem för informationssäkerhet	53
B 5 Personalsäkerhet	54
Före och i samband med anställning.....	55
Under anställning	56
Avslut eller ändring av anställning.....	56
B6 Leverantörsrelationer	57
B7 Efterlevnad och granskning	57
Kapitel C Informationssäkerhet i verksamhetsnära förvaltning	59
Inledning.....	60
Roller och ansvar	60
Systemägare	60

Systemförvaltare.....	60
Systemadministratör	60
Informationsägare	60
C 1 Dokumentation av informationssäkerhet.....	61
Systemsäkerhetsbeskrivning.....	61
C 2 Informationsklassning och systemklassning	62
C 3 Behörighetshantering och loggning.....	64
Logghantering	65
C4 Ändringshantering	66
C 5 Användarinstruktioner	67
C6 Riskanalys	67
C 7 Incidenthantering	68
C 8 Kontinuitetshantering	69
C 9 Kontroll av IT-tjänst	70
Kapitel D: Informationssäkerhet i IT-miljön.....	71
Inledning.....	73
Roller och ansvar	74
IT-säkerhetsansvarig	74
Rollen i den IT-nära förvaltningen	75
IT-chef och kontaktperson IT (Systemägare IT och systemförvaltare IT)	75
Ägare av IKT-objekt	75
Systemspecialister IT	75
Incidenthanterare - Incident manager	76
D1 Hantering av tillgångar	76
Identifiering av IT-resurser och tilldelning av ägare	76
Klassning av IT-resurser	77
Användningsinstruktioner.....	77
D2 Styrning av åtkomst	77
Identifiering och autentisering	79
Reglering av åtkomsträttigheter	79
Säkerhetsloggning.....	82
D3 Kryptering.....	83
D4 Fysisk och miljörelaterad säkerhet.....	83
Säkra utrymmen för IT-resurser	85
Godsmottagning och lastning.....	86

Underhåll, reparation och avveckling.....	86
Skydd av utrustning	86
Elförsörjning.....	87
D5 Driftsäkerhet	87
Säkerhetskopiering	88
Loggning och övervakning	90
Hantering av tekniska sårbarheter	91
D6 Kommunikationssäkerhet.....	91
Nätverkssäkerhet.....	92
Informationsöverföring.....	93
D7 Anskaffning och utveckling av IT-resurser	94
Säkerhetskrav på IT-resurser	94
Säkerhetskrav vid upphandling av IT-stöd.....	95
Säkerhet vid systemutveckling	97
Säkerhetskrav vid test	98
D8 Incidenthantering	99
Krisorganisation och krisplan.....	101
D9 Kontinuitetshantering	101
D10 Granskning och kontroll	102
Index – hänvisning till riktlinjetabeller.....	104
Revisionshistorik.....	106

Inledning

Norsjö kommuns informationssäkerhetspolicy är ett övergripande dokument som redovisar kommunens övergripande mål och inriktning med informationssäkerhet.

Riktlinjer för informationssäkerhet kompletterar informationssäkerhetspolicyen med mer detaljerad information och regler för hur information får hanteras inom kommunen.

Riktlinjernas omfattning

Dessa riktlinjer innehåller information och regler gällande säkerhet vid all hantering av information inom Norsjö kommun. Riktlinjerna gäller för alla verksamheter i Norsjö kommun, vilket medför att det inte finns utrymme att besluta om lokala regler som avviker från dessa.

Riktlinjerna gäller inte för kommunens bolag, utan dessa beslutar om informationssäkerhetspolicy och riktlinjer för informationssäkerhet inom egen verksamhet. I vissa fall kan ändå dessa riktlinjer gälla för kommunens bolag, liksom för andra externa aktörer, exempelvis när dessa använder sig av kommunens informationstillgångar, eller då det finns särskilda behov av samordning.

Dispenser och undantag

Ansökan om dispenser från dessa riktlinjer ska ställas till chef som tar upp till diskussion med IT-enheten. IT-enheten kan i sin tur ta upp diskussion i kommunens verksamhetsutvecklingsgrupp (VUG). Sådana ärenden ska beredas innan de ställs till IT-enheten för att underlätta beslut. Exempelvis kan en riskanalys ingå i beredningen av ärendet. Beslut om godkännande av undantag ska fattas av kommunchef efter beredning hos IT-enheten eller VUG, och i samråd med berörda.

Undantag från Riktlinjer för informationssäkerhet får aldrig vara permanenta utan ska ha en giltighetstid på som längst 2 år. Om behov av undantag kvarstår ska ärendet beredas på nytt och nytt beslut fattas om eventuellt godkännande.

Struktur och läsanvisningar

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

Kapitel		Innehåll	Primär målgrupp
A	Informationssäkerhet för medarbetare	Information och riktlinjer för hur information ska hanteras i olika situationer	Alla medarbetare
B	Styrning av informationssäkerhet	Ansvarsfördelning för informationssäkerhet. Information och riktlinjer för hur arbetet med informationssäkerhet ska bedrivas.	Verksamhetsansvariga, Informationsägare, alla som arbetar med IT-säkerhet, eller informationssäkerhet
C	Informationssäkerhet i verksamhetsnära förvaltning	Information och riktlinjer för informationssäkerhet i förvaltningsobjekt som t.ex system och grupper av system	Informationsägare, systemägare och systemförvaltare
D	Informationssäkerhet i IT-miljön	Information och riktlinjer för hur information och IT ska hanteras inom IT-miljön, dvs. IT- och cybersäkerhet.	Chefer och medarbetare på IT-enheten

Varje kapitel består både av informativa avsnitt och av riktlinjer som är obligatoriska.

Samtliga riktlinjer är numrerade och i tabellform med svart huvud. Rader som innehåller riktlinjer för konfidentiell information och höga skyddskrav har röda linjer, tjockare linje och nämnda termer är dessutom fetmarkerade. Exempel från Kapitel A om lagring i molntjänster:

Riktlinjer för lagring i molntjänster	
A 5.12	Norsjö kommuns information får <u>inte</u> lagras i <i>personliga</i> molntjänster (Onedrive, dropbox mfl).
A 5.13	Hög Sekretess (Röd) information får inte lagras i molntjänster

Andra tabeller, som inte innehåller riktlinjer utan är mer av illustrerande karaktär, har tabellhuvuden i annan färg.

Informationsklassning är en central del i kommunens arbete med informationssäkerhet och finns med genomgående i riktlinjerna. Hur information klassas ska styra i vilken grad informationen ska skyddas. Norsjö kommuns modell för informationsklassning beskrivs i Kapitel B och information och regler för hur information ska klassas och skyddas utifrån denna återfinns i respektive kapitel. Liksom vår informationssäkerhetspolicy är dessa riktlinjer baserade på den svenska och 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, ljud, bilder, film osv) och oavsett hur information 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 informationshantering handlar informationssäkerhet alltså om all information, oavsett form.

Detta inkluderar förutom information i IT-system även pappersbaserad information och information som finns i våra huvuden.

Information och de resurser som används för att hantera information benämns informationstillgångar. Informationssäkerhet utgörs av tre aspekter; att informationstillgångar ska vara konfidentiella, riktiga och tillgängliga (se Figur 1)

Figur 1



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 informationssäkerhet. Vad som är lämplig nivå av skydd för en viss informationstillgång beror på dessa krav, hotbild, 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 epostadress som mottagaren litar på i syfte att orsaka skada i någon form
IKT	Informations- och Kommunikationsteknik
Incident	Enskild eller flera oönskade eller oväntade händelser 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 (t ex öppen, känslig, sekretess)
Informationssäkerhet	Bevarande av informationens konfidentialitet, riktighet och tillgänglighet
Informationssäkerhetsincident	Enskild eller flera oönskade eller oväntade informationssäkerhetsincidenter 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 mm
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	Entydig 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, integritet och/eller tillgänglighet



Kapitel A: Informationssäkerhet för medarbetare

Inledning.....	14
A1 Övergripande regler.....	14
Medarbetares ansvar för informationssäkerhet.....	15
Skyldighet att rapportera incidenter och brister.....	16
Informationsklasser.....	17
Personuppgifter.....	19
Allmänna handlingar och sekretess.....	20
A 2 Lösenord.....	21
A3 E-post.....	23
A 4 Chatt/direktmeddelanden.....	25
A5 Lagring och säkerhetskopiering.....	25
Lagring på mobila enheter, smarta telefoner och surfplattor.....	28
A6 Mobila enheter (t ex bärbar dator, smarta telefoner, surfplattor).....	28
Särskilda regler för smarta telefoner och surfplattor.....	30
A7 Skadlig kod.....	31
Spridning av skadlig kod.....	32
A8 Internet och sociala media.....	32
A9 Spårbarhet och loggning.....	34
Rutin vid fördjupad granskning.....	35
Gallring av loggar från granskning.....	35
Pornografi.....	36

Anonymitetsserverar	36
Illegal fildelning.....	36
Rutin för loggning	36
Individuell loggning	37
Granskning av loggar	37
A10 Säkert beteende.....	37

Inledning

Detta kapitel vänder sig till alla medarbetare vid Norsjö kommun. Riktlinjerna gäller även extern personal som har åtkomst till Norsjö kommuns information, exempelvis inhyrda konsulter. Riktlinjerna beskriver det ansvar man som medarbetare har vid hantering av information i Norsjö kommun och vilka regler som gäller. Avvikelser från dessa riktlinjer får aldrig göras utan särskilt tillstånd. Kontakta ansvarig chef som i sin tur kontaktar IT-enheten vid osäkerhet om vad som gäller.

A1 Övergripande regler

Följande regler är övergripande och sammanställer grundläggande informationssäkerhetskrav på medarbetare:

Övergripande regler	
A 1.1	Medarbetare ska vara medveten om sin skyldighet att rapportera informationssäkerhetsincidenter och -brister i Norsjö kommuns informationshantering och IT-säkerhet. Detta ska göras till IT-enhetens support (via telefon eller besök) eller till närmaste chef. En incident som rör personuppgifter rapporteras till IT-enheten. Genom incidentrapporteringen har vi chans att förbättra vårt informationssäkerhetsarbete. En incident kan vara skadlig kod (virus), att personuppgifter har hamnat i orätta händer eller hanterats felaktigt, ett dataintrång eller stöld och förlust av utrustning innehållandes information.
A 1.2	Du som medarbetare har ansvar att kontrollera informationsklass så att du kan vara säker på att informationen får rätt skydd. Skyddet handlar till exempel om hur inloggning ska ske och hur säkerhetskopiering ska göras. Se stycke om de olika klasserna.
A 1.3	Lösenordet som medarbetare skapar för sin inloggning i Norsjö kommuns nätverk ska ha minst 16 tecken, innehålla en blandning av versaler, gemener, siffror och specialtecken. För övriga system gäller att säkert lösenord ska användas. Rådfråga gärna systemets förvaltare.
A 1.4	Det är otillåtet att dela på personliga konton. Varje individ måste kopplas till – och vara 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.

	Finns speciella behov så kontakta närmaste chef som har samråd med IT-enheten.
A 1.5	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.
A 1.6	Medarbetare får inte använda e-postadresser med domännamnet norsjo.se för privat bruk som registrering av ett privat konto i kommersiella tjänster. Sådan registrering kan medföra att Norsjö kommun kan få krav på att teckna företagslicens för nyttjande av tjänsten.
A 1.7	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.
A 1.8	Norsjö kommuns medarbetare ska följa svensk lag och kommunens interna riktlinjer vid internetanvändning.
A 1.9	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.
A 1.10	Medarbetaren ska ha kännedom om och tagit del av de styrdokument som berör medarbetarens arbete. Dessa finns publicerade på Norsjö kommuns intranät. Chef ansvarar för att ge medarbetare en introduktion till de styrande dokument som gäller.
A 1.11	Under distansarbete behöver du som medarbetare ta stort eget ansvar för att skydda kommunens information mot obehörig åtkomst. Chef ansvarar för att informera dig.

Medarbetares ansvar för informationssäkerhet

Information är en viktig resurs för Norsjö 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, vuxenutbildning, socialtjänst, hemsjukvård, samhällsplanering, biblioteksservice, bygglov med mera. 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 riktlinjer) eller fysiskt hur man skyddar utrymmen med dörrar, lås, skåp med mera. 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 Norsjö kommuns informationssäkerhet beror därför på hur den enskilde medarbetaren hanterar informationen och sin utrustning.

Norsjö kommun ställer krav på att medarbetare följer våra riktlinjer för informationssäkerhet. Chefer har ett ansvar att delge information och erbjuda utbildning i informationssäkerhetsfrågor till sina medarbetare. Som anställd på Norsjö 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 riktlinjer för informationssäkerhet följer Norsjö 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 misstänks kunna medföra negativ påverkan på kommunens information. Det kan röra sig om till exempel:

- IT-angrepp/intrång

- Skadlig kod
- Oskyddad känslig information
- Personuppgiftsincidenter
- Brister i efterlevnad av dessa riktlinjer för informationssäkerhet

IT-säkerhetsrelaterade incidenter och brister ska rapporteras till IT-enheten. Även incidenter angående personuppgifter ska rapporteras till IT-enheten. Gör anmälan via ett besök eller ett telefonsamtal. 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.

IT-enheten sammanställer incidenter och rapporterar vidare till kommunledningsgruppen 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.

Norsjö kommun anger i fyra klasser hur känslig informationen är och hur den får spridas: Öppen, Begränsad, Känslig-Sekretess eller Hög Sekretess. Information om dokumentets klassning kan lämnas i sidfot och i vissa fall i dokumenthanteringsplan. Informationsklasserna illustreras i Figur 2.

Informationsklass	Behörighet/spridning	Exempel
3 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. Medför allvarlig skada om informationen hanteras felaktigt.
2 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. Medför betydande skada om informationen hanteras felaktigt.
1 Begränsad (Grön)	Normal åtkomstbegränsning med viss spårbarhet	Allmänna personuppgifter, allmänna offentliga handlingar, födelsedata (6 första siffrorna i personnummer YYMMDD) Medför måttlig skada om informationen hanteras felaktigt.
0 Öppen (Vit)	Ingen åtkomstbegränsning	Handlingar utan direkta eller indirekta personuppgifter. Medför ingen eller försumbar skada om informationen hanteras felaktigt.

Figur 2 i Norsjö kommun används fyra informationsklasser

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.norsjo.se
- För Begränsad (Grön) information gäller normal åtkomstbegränsning och de normala hanteringsregler som finns nedan i avsnitt A1 – A9. 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. I detta kapitel är all information och alla riktlinjer som gäller för känslig information markerad med fetstil och med röda ramar i tabeller med riktlinjer. 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. Även dessa är markerade med fetstil, tjockare ram och röd ram.

Det finns dessutom information som är klassat högre än **Hög sekretess (Röd)**, sådan information regleras av säkerhetsskyddslagstiftning och är av betydelse för Sveriges säkerhet. Observera att särskilda regler finns för hantering av sådan information, kontakta Norsjö kommuns säkerhetsskyddschef eller kommunsekreterare.

Inom Norsjö kommun är idag långt ifrån all information klassad enligt de fyra klasserna men genom att du hanterar informationen enligt dessa klasser minskar risken för att personuppgifter och sekretessinformation hamnar fel.

Det viktigaste är att **Känslig-Sekretess (Gul)** och **Hög Sekretess (Röd)** information hanteras på rätt sätt. Det är bland annat känsliga personuppgifter och sekretessklassad information. Om du är osäker på hur viss information ska klassas och hanteras så fråga din chef, säkerhetsskyddschef eller kommunsekreterare.

Genom att tänka på hur anteckningar förs så går det undvika att skapa känsliga uppgifter i onödan. Genom att formulera sig på ett korrekt sätt kan en anteckning gå ifrån att vara sekretessklassad till att bli öppen.

Personuppgifter

Vid de flesta av Norsjö 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. till exempel får särskilt skyddsvärda personuppgifter inte skickas via okrypterad epost 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, till exempel utifrån krav från författningar.

Vid frågor om diarieföring, arkivering, utlämnande av handlingar så kontakta kommunkansliet.

A 2 Lösenord

Riktlinjer för utformning av lösenord	
A 2.1	Lösenord som du skapar för din inloggning till Norsjö kommuns nätverk ska vara minst 16 tecken långt. Till övriga system gäller att du ska ha säkert lösenord även om kravet inte alltid är 16 tecken.
A 2.2	Ett bra lösenord innehåller minst 1 stor bokstav, minst 1 liten bokstav, 1 siffra och minst 1 specialtecken
A 2.3	Lösenordet ska inte innehålla å, ä, ö, Å, Ä, Ö
A 2.4	Lösenordet får inte innehålla användarens inloggningsnamn, för- eller efternamn eller delar av namnet

Riktlinjer för hantering av lösenord

A 2.5	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-enheten för tips om sådana verktyg.
A 2.6	Samma lösenord ska inte användas privat och i jobbet. Olika lösenord ska dessutom användas för olika program och på olika tjänster på webben även om de är jobbrelaterade. På så vis minskas riskerna att någon kommer åt information.
A 2.7	Lösenord ska bytas direkt om misstanke finns att det har röjts.
A 2.8	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.
A 2.9	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.
A 2.10	Fundera gärna över vad det skulle innebära om ditt lösenord blev känt av andra. Vilka resurser skulle hen komma åt och vilken skada skulle det innebära. Tänk på att det är du som ansvarar för att ingen kommer åt information med hjälp av ditt lösenord.

För att logga in till de flesta av Norsjö 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. De flesta webbläsare har automatiska minnesfunktioner för att minnas de lösenord som du matar in. Ta för vana att inte spara lösenord i dina webbläsare med automatik eftersom då kan andra som har tillgång till din dator

logga in på dina sidor. De flesta webbläsare har en funktion där du kan ta bort sparade lösenord. Användar-ID och lösenord används för att skydda information som kan vara intern eller konfidentiell, och det är därför viktigt att följa nedanstående 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.

Tips: Ett sätt att skapa ett lösenord med bra kvalitet (starkt lösenord) kan vara att använda följande knep:

Skapa ett starkt lösenord genom att sätta ihop slumpmässiga ord tillsammans med siffror, specialtecken, stora och små bokstäver och är minst 12 tecken långt.

ex: kAtt1%Snarkar

Användar-ID och lösenord är i sig viktig information där Användar-ID är intern information medan lösenord är **känslig** information och ska hanteras på säkert sätt.

A3 E-post

E-post, ansvar	
A 3.1	Din personliga brevlåda fornamn.efternamn@norsjo.se är din tjänstbrevlåda
A 3.2	Den enskilde medarbetaren som är kontoinnehavare för ett personligt epostkonto är alltid ansvarig för den mejl som skickas från kontot
A 3.3	E-postkonton kan stängas vid misstanke om brott eller missbruk
A 3.4	E-postkonton som delas av flera, t.ex. myndighetsbrevlådor (för nämnder) och funktionsbrevlådor (t.ex. för enheter) ska ha utpekade ansvariga.
A 3.5	Mejl ska klassificeras utifrån dess innehåll. Använd den klassificeringsmodell som beskrivits i tidigare text.
A 3.6	Skriv inte känsliga uppgifter i ämnesraden, eftersom inkorgens register över inkomna e-postmeddelanden räknas som allmän handling.
A 3.7	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 avslöjas inte andras mejladresser vid "hemlig kopia"
A 3.8	Om du får hotelsebrev via mejl ska du spara mejlet och kontakta din chef

A 3.9	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.
-------	--

Privat e-post

A 3.10	Håll isär arbetsrelaterad och privat kommunikation när du kommunicerar via epost. Använd inte ditt epostkonto i Norsjö kommun för privata ändamål, utan ha en privat e-postadress som du inte använder för arbetsrelaterat material.
A 3.11	Det är inte tillåtet att automatiskt vidarebefordra din personliga e-postbrevlåda på kommunen till externa e-postadresser.

E-post och känslig information

A.3.12	Känslig – Sekretess (Gul) information får inte hanteras i Office365/Gmail.
A 3.13	Information som klassificerats som Hög sekretess (Röd) får inte hanteras i Office365/Gmail.
A 3.14	Dokument som skannas skickas ofta med mejl från skannern till mottagarens epostadress. Innan du skannar dokument som innehåller känslig - sekretess (gul) och Hög Sekretess (Röd) information bör du säkerställa att överföring sker på annat sätt än via vanlig e-post. Det finns särskilda verktyg för säker skanning. Kontakta IT-enheten vid frågor om säker skanning.
A 3.15	Om mejl <i>inkommer</i> 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.
A 3.16	Om mejl <i>inkommer</i> som innehåller Hög Sekretess (Röd) ska denna genast överföras till verksamhetssystem. Varpå meddelandet ska raderas från epostklienten.

E-post (mejl) 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.

A 4 Chatt/direktmeddelanden

Chat och känslig information

A.4.1	Känslig – Sekretess (Gul) information får inte hanteras i chatt.
A 4.2	Information som klassificerats som Hög sekretess (Röd) får inte hanteras i chatt.
A 4.3	Om chatt <i>inkommer</i> 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 (Teams, Messenger eller liknande) 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.

A5 Lagring och säkerhetskopiering

Riktlinjer för lagring och säkerhetskopiering

A 5.1	Kommunens information ska lagras i kommunens tillhandahållna tjänster på så sätt att den finns tillgänglig för den som behöver den.
A 5.2	Om information i undantagsfall behöver lagras på lokal hårddisk, se till att regelbundet kopiera över informationen till din nätverksyta (W:) eller till din OneDrive kopplat till ditt kommunkonto. Om hårddisken på din dator kraschar kommer annars informationen att vara förlorad.
A 5.3	Om information på nätverket eller i din OneDrive har gått förlorad, exempelvis om man av misstag råkat radera ett dokument, ska IT-enheten kontaktas, förhoppningsvis kan de då återskapa den senaste säkerhetskopian.

A 5.4	Känslig- Sekretess (Gul) information ska i första hand lagras i verksamhetssystem
A 5.5	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.
A 5.6	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.
A 5.7	Lokal lagring (synkronisering) av Känslig – Sekretess (Gul) information, t.ex. på en persondator, får endast ske på en krypterad kommunägd dator.
A 5.8	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 Norsjö kommun tillhandahåller. Kontakta IT-enheten. USB minnet ska förvaras betryggande då det inte används. Vid osäkerhet, kontakta IT-enheten.
A 5.9	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 med mera. Om du är osäker på hur din information säkerhetskopieras så kontakta IT-enheten.

Riktlinjer för lagring i molntjänster

A 5.10	Endast godkända molntjänster är tillåtna att användas. Du ansvarar för att kontrollera vilka molntjänster som är tillåtna inom din verksamhet
A 5.11	Som användare ska du inte koppla en molntjänst du använder privat till din kommunala e-postadress.

A 5.12	Norsjö kommuns information får <u>inte</u> lagras i <i>personliga</i> molntjänster (Dropbox mfl).
A 5.13	Hög Sekretess (Röd) information får inte lagras i molntjänster

Riktlinjer för lagring i OneDrive/SharePoint Online

A 5.14	Du ansvarar för att allmänna handlingar tas om hand för registrering och arkivering, och att information i din OneDrive gallras enligt fastställda dokumenthanteringsplaner.
A 5.15	Känslig Sekretess (Gul) och Hög Sekretess (Röd) information får inte lagras i OneDrive eller SharePoint Online av juridiska skäl. På OneDrive sparar du annat material som du lätt vill komma åt att redigera när som helst, var som helst. Det är i OneDrive du har dina egna arbetsrelaterade dokument. Via OneDrive kan du dela ett dokument med en eller ett par kollegor om du behöver synpunkter eller dialog kring ett innehåll.
A 5.16	Använd inte OneDrive för information som din <i>arbetsgrupp eller flera användare</i> behöver ha åtkomst till. Gemensamt material kan delas via SharePoint Online eller annan lagringsplats. Arbetsgruppens filer kan sparas i Teams. Kontakta din chef för att få information om vilka samarbetsytor ni använder er av.
A 5.17	När din anställning ska avslutas ansvarar du för att information som finns på din OneDrive och som kan vara av vikt för din arbetsplats, lagras på annan lagringsplats.

Riktlinjer för lagring i G Drive (Utbildning)

A 5.18	Du ansvarar för att allmänna handlingar tas om hand för registrering och arkivering, och att information i din G Drive gallras enligt fastställda dokumenthanteringsplaner.
A 5.19	Känslig Sekretess (Gul) och Hög Sekretess (Röd) information får inte lagras i G Drive av juridiska skäl. När din anställning ska avslutas ansvarar du för att information som finns på din G Drive, och som kan vara av vikt för din arbetsplats, lagras på annan lagringsplats

Molntjänster är datortjänster som tillhandahålls över Internet, exempelvis lagring eller programvaror. Office 365 är ett exempel på molntjänster som Norsjö kommun valt att införa.

Lagring på mobila enheter, smarta telefoner och surfplattor

Se avsnitt Mobila enheter

A6 Mobila enheter (t ex bärbar dator, smarta telefoner, surfplattor)

Riktlinjer för hantering av mobila	
A 6.1	Känslig och sekretessinformation måste vara krypterad och får enbart hanteras på av IT-enheten managerade mobila enheter. Detta sköts automatiskt om du har en av IT-enheten managerad enhet.
A 6.2	Mobila enheter ska låsas med lösenord eller liknande.
A 6.3	Mobila enheter som tillhandahålls av Norsjö kommun är personliga arbetsredskap och får inte lånas eller överlåtas om det inte är enheter som delas av flera.
A 6.41	Innan receptionen lämnar ut en smart telefon hanterar IT-enheten den via Intune genom att lägga in exempelvis den programvara du har rätt att använda.
A 6.42	Under en övergångsperiod kommer redan driftsatta smarta telefoner att hanteras på ett enklare sätt.
A 6.5	Uppsatta säkerhetsinställningar i enheter får inte ändras.
A 6.6	Om du är i behov av ytterligare programvaror eller hårdvara ska du anmäla det till din närmaste chef.
A 6.7	Viktig information bör inte lagras enbart på en bärbar enhet, i så fall ska den snarast kopieras över till kommunens nätverk och där det är möjligt till aktuellt verksamhetssystem så att informationen erhåller rätt skydd.
A 6.8	Kommunenheter som används ute i verksamheterna får enbart anslutas till nätverk som är "vitlistade" av IT-enheten och som är lösenordskyddade. Om du besöker annan plats så var försiktig med att ansluta till "öppna" nät till exempel på hotell, caféer, tåg eller flygplan. Om du ställs inför en situation där det inte finns ett vitlistat nätverk, och du känner osäkerhet, så kontakta IT-enheten för råd.

	Vid distansarbete avgör din chef om din anslutning kan anses vara godkänd.
A 6.9	<i>Privat utrustning</i> kan i vissa fall användas men följ de instruktioner som ges av chef i samråd med IT-enheten. Privat utrustning bör ej anslutas till annat än kommunens gästnät. Privat utrustning som inte manageras via IT-enheten får aldrig användas för känslig eller sekretessinformation.
A 6.10	Försiktighet ska iakttas vid mobilt arbete i publika miljöer, exempelvis kan skärmen på enheten skyddas med insynsskydd (s.k. sekretesskydd).
A 6.11	Arbete med Känslig – Sekretess (Gul) och Hög sekretess (Röd) information får inte ske i publika miljöer. Om man som anställd absolut måste behandla känslig information i publika rum som till exempel hemma hos en brukare eller på ett bibliotek är det viktigt att göra det på ett sådant sätt att risken för att känslig information sprids till obehöriga elimineras.
A 6.12	Mobila enheter får inte lämnas utan uppsikt och ska förvaras i säkert och skyddat utrymme.
A 6.13	Förlust av mobil enhet ska omedelbart anmälas till receptionen, detta ska göras innan polisanmälan. I många fall finns möjligheter att fjärradera information.
A 6.14	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-funktionen.
A 6.15	Utrustningen ska i övrigt vårdas och hanteras på det sätt som föreskrivs, till exempel skyddas mot värme och fukt samt hållas uppdaterad.
A 6.16	Vid service ska den mobila enheten inlämnas enligt fastställda rutiner som receptionen informerar om.
A 6.17	Om utrustningen måste lämnas in för service så ska du försäkra dig om att den inte innehåller känslig- eller sekretessinformation

Den IT-utrustning som tillhandahålls av Norsjö 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 riktlinjer utöver dessa som presenteras här. Kolla med din chef om du är osäker vad som gäller.

Särskilda regler för smarta telefoner och surfplattor

Regler för smarta telefoner och surfplattor	
A 6.19	<p>Norsjö kommun äger mobiltelefoner och surfplattor som tillhandahålls för arbetet. Norsjö kommun är alltså ägare till den arbetsrelaterade informationen som finns i dessa enheter.</p> <p>Enligt offentlighetsprincipen kan det också vara möjligt för allmänheten att begära ut allmänna handlingar, till exempel <u>arbetsrelaterade</u> SMS eller bilder, som förvaras på telefonen/surfplattan.</p>
A 6.20	<p>Det finns ett stort utbud av appar att ladda ner. Många av dessa appar kan innehålla skadlig kod, använd därför endast godkända appar.</p> <p>Varje telefon som lämnas ut av receptionen ska vara registrerad hos IT och godkända appar installerade. Om en telefon misstänks vara felaktigt registrerad eller användas felaktigt, har IT rätt att blockera telefonen.</p>
A 6.21	<p>Norsjö kommuns information kan inte hanteras i smart telefon eller surfplatta om inte särskild av kommunen godkänd säkerhetslösning används på grund av risk för informationsläckage.</p>
A 6.22	<p>För utrustning som lämnats ut av Norsjö kommun gäller att pinkod (6 siffror), fingeravtryck eller annan autentisering måste användas. 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.</p>
A 6.23	<p>Vårda utrustningen och använd exempelvis skärmskydd och skal.</p>
A 6.24	<p>Huvudregeln är att vid anställningens upphörande ska surfplattan och/eller den smarta telefonen återlämnas till närmaste chef som i sin tur kontaktar IT-enheten.</p>
A 6.25	<p>Vid längre tjänstledighet kan telefonen behöva lämnas åter, det avgör närmaste chef.</p>

A 6.26	I de fall det krävs multifaktorinloggning till kommunens IT-resurser är en smart telefon ett viktigt verktyg – därför måste din smarta telefon hanteras som en värdehandling.
A 6.27	Du kan få tillstånd att nyttja din arbetsmobil privat. Detta tillstånd ges av chef i samråd med IT-enheten. Följ din chefs instruktioner angående hur du får använda den utanför arbetstid.

A7 Skadlig kod

Riktlinjer för skydd mot skadlig kod

A 7.1	Stäng aldrig av eller på annat sätt inaktivera installerat skydd mot skadlig kod
A 7.2	Anslut endast arbetsrelaterad IT-utrustning till kommunens administrativa nätverk
A 7.3	Var misstänksam och undvik att klicka på konstiga länkar eller fylla i kontouppgifter
A 7.4	Öppna bifogade filer endast om de kommer från en känd avsändare och en bilaga är förväntad. Är du osäker, ring avsändaren och fråga.
A 7.5	Var observant på om IT-utrustning betar sig långsamt eller konstigt. Vid misstanke om skadlig kod, gör så här: 1) koppla ifrån wifi/dra ur nätverkskabeln 2) låt datorn vara på 3) kontakta IT-enheten. OBS! Anmälan till IT-enheten 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, så som 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 så kallat 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! Seriosa 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. Alla medarbetare kan också bidra till ett bra skydd mot skadlig kod genom att följa dessa regler:

A8 Internet och sociala media

Riktlinjer för internetanvändning	
A 8.1	Internet är i arbetet på Norsjö kommun främst ett arbetsverktyg och ska inte störa ordinarie arbetsuppgifter eller innebära merkostnader för kommunen.
A 8.2	Det är tillåtet att använda Internet för privat bruk under egenansvar om det inte inkräktar på arbetet eller medför kostnader för kommunen. Kommunen förutsätter att den som surfar på Internet endast besöker lagliga webbplatser.
A 8.3	Utrymmeskrävande filtyper inklusive filmer, program och spel får dock inte för privat bruk laddas ned, strömmas, lagras eller spridas i, eller via, Norsjö kommuns nätverk.
A 8.4	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

A 8.5	Norsjö kommun har ett filter för att i förebyggande syfte förhindra oetisk internetsurfning och direkt brottslig verksamhet. I samband med finns även möjlighet till loggning av Internettrafik. Loggningen ska kunna tillhandahålla material som krävs för att bevisa eller motbevisa påståenden och misstankar om brottslig eller otillbörlig användning av Internet som anställd vid Norsjö kommun
A 8.6	De regler som gäller i samhället i övrigt gäller självklart även inom Norsjö kommun. Tryckfrihetsförordningen, brottsbalken, lagen om upphovsrätt samt lagar som reglerar personuppgiftsbehandling är exempel på lagar som ibland måste beaktas när man använder Internet
A 8.7	För material på Internet som ska användas i tjänsten, får nedladdning och installation av upphovsrättsligt material (dator, film, musik, m.m.) inte ske utan stöd i lag, avtal eller med skriftligt tillstånd från rättighetsinnehavaren.
A 8.8	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 riktlinjer som är kopplade till skadlig kod i avsnitt A7 finns här särskilda regler för användning av Internet och sociala medier.

Etiska riktlinjer

A 8.9	All kommunikation på Internet från Norsjö 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
A 8.10	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 Norsjö kommun som organisation. Det är därför särskilt viktigt att som representant för Norsjö kommun beakta god etik och gott omdöme på Internet. Norsjö kommuns regler och värderingar ska följas även vid kommunikation via Internet och sociala medier.

Riktlinjer vid användning av sociala medier

A 8.11	Vid användning av sociala medier, se till så att det inte framstår som om åsikter som uttrycks är Norsjö kommuns.
A 8.12	Det är viktigt att du skiljer på vad du gör i sociala medier som privatperson och som representant för Norsjö kommuns verksamheter.
A 8.13	Du har självklart rätt att diskutera Norsjö 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.
A 8.14	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.
A 8.15	Gör du inlägg eller kommenterar med Norsjö kommuns profil/användare så representerar du Norsjö kommun. Skriver du med ditt eget användarkonto och profil som avsändare gör du det som privatperson.
A 8.16	I ditt personliga konto får du inte använda bilder och filmer som tillhör Norsjö kommun utan att fråga fotografen först. Att dela inlägg med kommunalt material från kommunal avsändare är däremot givetvis helt okej.

Norsjö kommun är aktivt på sociala medier. Den personal som är utsedda att skriva i Norsjö kommuns namn har särskilda regler och kunskap om kommunikation.

A9 Spårbarhet och loggning

Riktlinjer för granskning av loggar

A 9.1	Materialet får inte användas av arbetsgivaren i allmänt kontrollerande syfte.
A 9.2	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:

Riktlinjer för fördjupad granskning	
A 9.3	Vid granskningen skall alltid två personer närvara
A 9.4	Verksamhetschef utser person från verksamheten och IT-chef utser teknisk assistans. Personerna får endast tillgång till loggarna i samband med granskningen.
A 9.5	Granskningen ska genomföras skyndsamt och enligt fastställd teknisk rutin
A 9.6	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

Riktlinjer för gallring av loggar från granskning	
A 9.7	Granskningsloggar ska raderas efter ärendet är avslutat
A 9.8	Undantag ska göras för loggar som påvisat brottslig aktivitet eller brott mot regler samt loggar som berörs av påbörjad undersökning
A.9.9	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. Norsjö kommun kan, utan att meddela användaren, gå igenom dessa loggar för att kontrollera efterlevnad av lagstiftning och riktlinjer. Vid misstanke om brott kan loggfilerna komma att lämnas ut till rättskipande myndighet utan att du som kontoinnehavare meddelas.

Om användare, via Internet, surfar in på en webbsida eller annat tillgängligt som finns definierat som förbjudet i de tabeller som styr filtret, får användaren ett meddelande att denne nekas tillträde till sidan. Användaren får också ett meddelande att han/hon försökt nå en förbjuden adress.

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.

Granskning av loggar

Direkt granskning av loggar får endast ske när det finns anledning misstänka att överträdelser sker.

A10 Säkert beteende

Riktlinjer för muntlig information	
A 10.1	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 arbetsituationer 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.
A 10.2	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
A 10.3	Endast öppen information ska kommuniceras hörbart utanför arbetsplatsen, exempelvis vid fysiska samtal på tåget, eller i telefonsamtal i kassakön.
A 10.4	För videomöten gäller att Känslig – Sekretess (Gul) och Hög Sekretess (Röd) endast får förekomma i funktion för säkra videomöten, Vidicue.

Riktlinjer för information på skärmar och i pappersform

A 10.4	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.
A 10.5	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 sk smart kort till datorn (SITHS eller liknande) ska detta tas ut då man lämnar arbetsplatsen.
A 10.6	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. Anställd möblerar sitt kontor så att insyn på skärm genom fönster eller dörr förhindras.
A 10.7	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.
A 10.8	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). Om externbrev innehåller Hög Sekretess (Röd) information, använd särskilda säkerhetspåsar för försändelser.
A 10.9	Fax är ett väldigt osäkert kommunikationssätt, och ska undvikas i största möjliga mån. 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.

A 10.10	Fax får inte användas till Hög Sekretess (Röd) information
A 10.11	Vid utskrift ska dokument omgående hämtas upp ur skrivare. Vid utskrift av Känslig – Sekretess (Gul) och Hög Sekretess (Röd) information måste extra försiktighet iakttas. 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. Kontakta IT-avdelningen vid frågor.
A 10.12	Hög Sekretess (Röd) måste vid kassering strimlas i för klassen godkänd storlek och kastas i godkända säkerhetskärl. Begränsad (Grön) och Känslig – Sekretess (Gul) måste vid kassering strimlas.

En stor del av kommunens information hanteras muntligt och på papper. Vi kommunicerar dagligen informellt och formellt på detta sätt och vi måste bete oss särskilt försiktigt då vi hanterar **Känslig – Sekretess** (Gul) eller **Hög sekretess** (Röd) information.

Tänk på att det alltid finns informell information som inte i förhand är definierad och klassad, utan som skapas i det ögonblick det uttalas eller skrivs. Det kan vara till exempel omdömen om chefer och medarbetare – skvaller, rykten med mera – eller information om en oförutsedd händelse, till exempel ett brott.

Sådan information kan vara känslig och är i så fall att betrakta som **Känslig – Sekretess** (Gul) information.

B

Kapitel B Styrning av informationssäkerhet

Inledning.....	42
B1 Roller och ansvar	42
Grundprincip.....	42
Kommunfullmäktiges ansvar	42
Kommunstyrelsens ansvar.....	42
Ansvar inom varje utskott och dess verksamheter.....	43
Medarbetares ansvar	43
Personuppgiftsansvar	43
Arkivmyndigheten.....	44
Systemägares ansvar	44
Ansvar i projekt	44
IT-enhetens ansvar	44
IT-säkerhetsansvarig.....	45
CISO.....	45
Beredskap/räddningstjänst.....	45
Digitaliseringsgruppen - Informationsforum	45
Dataskyddsombud	46
Kommunens revisorer	47
B2 Dokumentstruktur	47

B3 Informationsklassning.....	49
Vad ska klassificeras?	52
Användningsområden och målgrupper	52
B4 Ledningssystem för informationssäkerhet	53
B 5 Personalsäkerhet	54
Före och i samband med anställning.....	55
Under anställning	56
Avslut eller ändring av anställning.....	56
B6 Leverantörsrelationer	57
B7 Efterlevnad och granskning	57

Inledning

Detta kapitel beskriver och reglerar hur arbetet med informationssäkerhet ska bedrivas i Norsjö 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 verksamheter, projekt eller. Kapitlet kan även vara informativt för andra som är intresserade av hur arbetet med informationssäkerhet bedrivs i Norsjö 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 Norsjö kommun antagit i och med dessa riktlinjer.

B1 Roller och ansvar

Grundprincip

Ansvaret för informationssäkerheten följer det ordinarie verksamhetsansvaret. Detta gäller från styrelse/utskott till den enskilde medarbetaren. 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 informationssäkerhetsgrupp, dataskyddsombud, beredskapssamordnare, digitaliseringsstrateg, kommunstrateg och övriga som arbetar specifikt med informationssäkerhet, IT-säkerhet eller andra relaterade frågor fungerar som stöd till medarbetare, verksamheter och kommunens ledning 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. Kommunchef har ansvar för att informationssäkerhetsarbetet bedrivs i linje med den av kommunfullmäktige fastställda informationssäkerhetspolicy. Kommunstyrelsen fastställer kommunövergripande riktlinjer för informationssäkerhet.

Ansvar inom varje utskott och dess verksamheter

Varje utskott, via KS, ansvarig för informationssäkerheten inom sitt verksamhetsområde. Verksamhetsansvarig, oavsett nivå, ansvarar för informationssäkerheten inom sin verksamhet. Verksamhetsledningen ansvarar för att verksamhetens medarbetare känner till och efterlever informationssäkerhetspolicyn och riktlinjer 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 riktlinjer för informationssäkerhet samt eventuella verksamhets-specifika 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.

Riktlinjer för medarbetare återfinns i Kapitel A.

Personuppgiftsansvar

Kommunstyrelsen är personuppgiftsansvariga. Som personuppgiftsansvariga har de det yttersta ansvaret för all behandling av personuppgifter och informationssäkerheten knuten till den behandlingen. Till stöd finns dataskyddsombud som samordnar personuppgiftshanteringsarbetet i enlighet med lagstiftning och kommunens interna bestämmelser.

Dataskyddsombudet är ett rådgivande och samordnande stöd till verksamhetens ledning i verksamhetens interna informationssäkerhetsarbete kopplat till personuppgiftshantering. 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. Norsjö kommuns dataskyddsombud fås via köpt tjänst från Skellefteå kommun.

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.

Arkivmyndigheten

Kommunstyrelsen är kommunens arkivmyndighet. Arkivmyndigheten utövar tillsyn över att kommunens myndigheter fullgör sina skyldigheter beträffande arkivbindningen och dess syften samt över arkivvården i kommunen. Hos arkivmyndigheten finns ett centralarkiv. Kommunkansliet är arkivmyndighetens operativa organ och ger råd och anvisningar om arkivvård och dokumenthantering.

Systemägares ansvar

Systemägare ansvarar för att den som använder systemet efterlever informationssäkerhetspolicy och riktlinjer för informationssäkerhet. En viktig del i ansvaret är att besluta om informationens/systemets informationssäkerhetsnivåer genom att klassning sker i enlighet med Norsjö kommuns modell för informationsklassning. Informationssäkerhetsansvar hos övriga roller inom förvaltningsorganisationen beskrivs i Kapitel C.

I den mån det inte finns utpekade systemägare följer ansvaret verksamhetsansvaret. Riktlinjer för informationssäkerhet i verksamhetsnära förvaltning återfinns i Kapitel C.

Ansvar i projekt

Verksamheten äger projektet via en utsedd projektägare som säkerställer att säkerhetsfrågorna beaktas. Styrgruppen är ansvarig för att säkerhetsfrågorna beaktas och ska tillsammans med projektägaren fastställa säkerhetsnivån för det som utvecklas. Under projektets gång ska styrgruppen följa upp hanteringen av de säkerhetsrelaterade frågorna.

Projektledaren ansvarar för att fastslagen säkerhetsnivå beaktas i projektarbetet.

IT-enhetens ansvar

IT-enhetens ansvarar för den tekniska säkerheten i kommunens IT-miljö som tjänster, processer, system, infrastruktur, verktyg etc och att den är robust, tillräcklig och

uppfyller verksamhetens krav, legala krav samt informationssäkerhetspolicy och riktlinjerna för informationssäkerhet.

CISO (chief information security officer)

CISO utses av kommunchef. CISO samordnar arbetet med säkerheten i Norsjö kommuns IT- miljö och är stödjande vid kravställning på externa aktörer. Rollen beskrivs utförligare i Kapitel D.

Informationssäkerhetsarbetet i kommunen leds och samordnas av CISO.

Hen ansvarar för:

- att kommunens styrande dokument inom området är aktuella, som informationssäkerhetspolicy och riktlinjer 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 samarbeta med dataskyddsamordnaren i informationssäkerhetsfrågor
- kontroll och uppföljning av informationssäkerheten,
- omvärldsbevakning inom informationssäkerhetsområdet,

Beredskap/räddningstjänst

Räddningstjänsten har uppdraget att utöva kommungemensam styrning av säkerhetsarbetet. Varje styrelse/utskott ansvarar för säkerhets- och trygghetsarbetet inom sitt område och sina respektive verksamheter.

Räddningstjänst/beredskapssamordnare ska verka som en organiserande och koordinerande process i kommunens säkerhetsarbete och ska stödja verksamheterna och de kommunala bolagen i deras säkerhetsarbete.

Informationssäkerhetsgruppen - Informationsforum

Gruppen är en kommunövergripande grupp som utses och leds av CISO. Som utgångspunkt ingår: IT-säkerhetsansvarig, inköp, registrator, kommunsekreterare och digitaliseringsamordnare i gruppen. Vid behov ska även andra kompetenser bjudas in.

En gång per år tar informationssäkerhetsgruppen fram en rapport som lämnas till ledningsgruppen tillsammans med ett erbjudande om muntlig presentation för att ge en beskrivning av informationssäkerhetsläget.

Ansvar för informationssäkerhet följer med verksamhetsansvaret och varje verksamhet är därmed ansvarig för sin egen informationssäkerhet. Gruppen fungerar endast som rådgivande och bollplank till CISO som ska fatta beslut om frågor som rör informationssäkerhet.

Exempel på områden där informationssäkerhetsgruppen kan agera bollplank

- frågor som gäller undantag från kommunens riktlinjer för informationssäkerhet
- frågor om specifika informationssäkerhetslösningar,
- frågor om Informationssäkerhetspolicyn och riktlinjer för informationssäkerhet
- frågor om systemklassning.

Dataskyddsombud

Dataskyddsombudets uppgift, via dataskyddssamordnaren, 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 och dataskyddssamordnaren ska stödja dataskyddsombudet i dennes utförande av dessa uppgifter.

Dataskyddsombudet ska, via dataskyddssamordnaren, på begäran ge råd om konsekvensbedömningar avseende dataskydd och övervaka genomförandet av konsekvensbedömningen.

Dataskyddsombudet ska samarbeta med tillsynsmyndigheten och vid behov fungera som kontaktpunkt för tillsynsmyndigheten. Dataskyddsombudet ska, via dataskyddssamordnaren, 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 dataskyddsförordningen.

Kommunens revisorer

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

B2 Dokumentstruktur

Riktlinjer för dokumentstruktur för informationssäkerhet	
B 2.1	Norsjö 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.
B 2.2	Handlingsplaner för informationssäkerhet ska tas fram med jämna mellanrum baserade på informationssäkerhetsanalyser
B 2.3	Det ska finnas en för Norsjö kommun övergripande informationssäkerhetspolicy som uttrycker ledningens viljeinriktning med informationssäkerhet
B 2.4	Det ska finnas kommunövergripande riktlinjer för informationssäkerhet som konkretiserar informationssäkerhetspolicy och som riktar sig till relevanta målgrupper
B 2.5	Det ska finnas modeller, metoder, vägledningar och andra stöddokument som stödjer olika gruppers efterlevnad av informationssäkerhetspolicy och riktlinjerna för informationssäkerhet

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

Informationssäkerhetspolicy

Riktlinjer för informationssäkerhet (*detta dokument*)

Informationssäkerhetsanalys (-er)

Handlingsplan för informationssäkerhet

Informationssäkerhetspolicy och Riktlinjer för informationssäkerhet (*detta dokument*) riktar sig till alla medarbetare och politiker inom Norsjö kommun.

Informationssäkerhetspolicyn är ett övergripande dokument som uttrycker kommunstyrelsens viljeinriktning med informationssäkerhet. Beslutas av Kommunfullmäktige och uppdateras vid behov.

Riktlinjer för informationssäkerhet (detta dokument) innehåller riktlinjer för hantering av information. Riktlinjerna är uppdelade i kapitel för olika målgrupper.

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

Informationssäkerhetsanalysen är en genomlysning av informationssäkerheten i Norsjö kommun innefattande hotbild, skydds nivåer, 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 med jämna mellanrum och innehåller konkreta mål och åtgärder baserade på informationssäkerhetsanalysen.

Se figur 3.

Figur 3



Modeller, metoder, vägledningar och andra stöddokument kan tas fram centralt för att stödja arbetet med informationssäkerhet på olika nivåer och att underlätta tillämpningen efterlevnaden av informationssäkerhetspolicyn och riktlinjerna för informationssäkerhet.

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

B3 Informationsklassning

Riktlinjer för informationsklassificering	
B 3.1	Det ska finnas en kommungemensam modell för informationsklassificering
B 3.2	Norsjö 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 Norsjö kommuns verksamheter.

Att klassificera information på ett enhetligt sätt utifrån konfidentialitet, riktighet och tillgänglighet är en fundamental aktivitet i en metodbeskrivning, dvs ett ledningssystem för informationssäkerhet (LIS). Det är också en rekommendation från MSB – Myndigheten för samhällsskydd och beredskap – att organisationer ska klassa sin information och bygga sina säkerhetsåtgärder utifrån klasserna. En klassningsmodell definierar nivåer av skydds krav kopplat till de tre aspekterna konfidentialitet, riktighet och tillgänglighet så att information kan klassas på ett enhetligt sätt i hela organisationen.

Norsjö kommun har i och med dessa riktlinjer antagit en modell för informationsklassning, se tabell. 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 Norsjö kommun, enskilda individer (fara för liv) eller andra organisationer. (I KLASSA: Nivå 3 allvarlig skada)
2 Höga skyddskrav	Känslig – sekretess -information som om den sprids till obehöriga kan medföra betydande negativ effekt för Norsjö kommun, enskilda individer eller andra organisationer. (I KLASSA: Nivå 2 betydande skada)
1 Normala skyddskrav	Begränsad information som om den sprids till obehöriga kan medföra måttlig negativ effekt för Norsjö kommun, enskilda individer eller andra organisationer. (I KLASSA: Nivå 1 måttlig skada)
0 Inga skyddskrav	Öppen information som kan spridas fritt inom och utom Norsjö kommun. (I KLASSA: Nivå 0 ingen eller försumbar skada)

OBS! Det finns dessutom information som är klassat högre än **Hög sekretess (Röd)**, sådan information regleras av säkerhetsskyddslagstiftning. I KLASSA är det nivå 4, av betydelse för Sveriges säkerhet.

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.

Figur 5

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. Individens 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:

Informationstyp	Konfidentialitet	Riktighet	Tillgänglighet
Öppettider badhus	0	1	1
Personaluppgift (exkl adress)	1	1	1
Personaluppgift med adress	2	1	1
Personaluppgift för medarbetare inom sociala	3	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, exvis SITHS-kort, BankID, 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 och systemförvaltare är därför att klassa sina system så att rätt skyddskrav erhålls. Riktlinjer för detta finns i Kapitel C.

Riktlinjer för informationssäkerhet i verksamhetsnära förvaltning återfinns i Kapitel C

Informationsklassning har ännu inte påbörjats i Norsjö kommun. Målsättningen är främst att inleda klassning av kritisk information som har höga skyddskrav för en eller flera av aspekterna konfidentialitet, riktighet och tillgänglighet.

Användningsområden och målgrupper

Modellen vänder sig dels till de i Norsjö kommun som är verksamhetsansvariga och/eller ägare av information och system/program, 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 informations-säkerhetsbehovet 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 (Figur 2 och figur 4). En mer utförlig vägledning som stöd för informationsklassning avses att skapas i framtiden.

B4 Ledningssystem för informationssäkerhet

Riktlinjer för ledningssystem för informationssäkerhet (LIS)

B 4.1	Norsjö kommun designar och inför ledningssystem för informationssäkerhet.
-------	---

I Norsjö kommuns informationssäkerhetspolicy anges att man ska bedriva ett systematiskt informationssäkerhetsarbete.

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. I Norsjö är LIS i form av en metodbeskrivning för vårt arbete med informationssäkerhetsarbete.

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 Norsjö kommuns arbete med att skapa ett LIS ingår dessa riktlinjer där roller, ansvar och informationsklassning är viktiga element. Att arbeta ett LIS är ett levande arbete och kommer att fortgå under ett antal år framåt.

Ett ledningssystem för informationssäkerhet bör utgå 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.**

Arbetet med metodbeskrivning för informationssäkerhetsarbete i form av ett LIS för Norsjö kommun bör fortgå och förfinas av informationssäkerhetssamordnare. Detta bör omfatta samtliga delar av informationssäkerhetsarbetet i kommunen.

B 5 Personalsäkerhet

Riktlinjer för personalsäkerhet före och i samband med anställning	
B 5.1	Bakgrundskontroll av sökande ska göras före anställning där sökandes meritförteckning kontrolleras.
B 5.2	Anställning av kritiska roller ska genomgå förstärkt kontroll. Detta kan vara i form av kreditupplysning och kontroll i brottsregister. Vid osäkerhet, kontakta personalenheten.
B 5.3	För befattningar som har betydelse för Sveriges säkerhet, och som omfattas av Säkerhetskylldslagen (2018:585) ska det i anställningsförfarandet genomföras en registerkontroll. Säkerhetsfunktion via räddningschef beslutar om detta.
B 5.4	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 riktlinjer. Och annat ansvar som följer med rollen, t.ex. systemägarskap och systemförvalterskap.
B 5.5	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.

Riktlinjer för personalsäkerhet under anställning	
B 5.6	Alla medarbetare och i förekommande fall externa aktörer ska erhålla lämplig utbildning för att kunna efterleva kommunens informationssäkerhetspolicy och riktlinjer för informationssäkerhet.
B 5.7	Roller som har särskilda uppgifter inom informationssäkerhet ska få lämplig fortbildning inom området som är relevant för deras befattning
B 5.8	Arbetsrättsliga åtgärder kan behöva vidtas då anställda har brutit mot gällande informationssäkerhetsregler.

Riktlinjer för personalsäkerhet för avslut eller ändring av anställning

B 5.9	Ansvar och skyldigheter för informationssäkerhet som förblir gällande efter avslut eller ändring av anställning ska definieras och kommuniceras vid anställningstillfället eller tillträddande av roll och framgå i sekretessförbindelse.
B 5.10	Återlämnande av IT-resurser och indrag av åtkomsträttigheter till information och IT-resurser ska ske i direkt samband med avslut eller ändring av anställning.
B 5.11	Närmaste chef är ansvarig för att avbeställa behörigheter, passerkort, utrustning, smarta kort (SITHS) mm utifrån fastställda rutiner som gäller vid avslutning av anställning.
B 5.12	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) mfl.

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

Nyanställda ska delges ansvar och skyldigheter kopplade till informationssäkerhet och genomgå utbildning i informationssäkerhet samt ta del av informationssäkerhet för medarbetare enligt dessa riktlinjer. Delgivning och utbildning ska också ges kopplat till annat ansvar som följer med rollen, till exempel informationsägarskap.

Under anställning

I enlighet med informationssäkerhetspolicy 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 riktlinjer 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 misshandling.

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 anställda haft tillgång till konfidentiell information. Detta ska definieras och kommuniceras till den anställda vid anställning/tillträddande 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.

B6 Leverantörsrelationer

Riktlinjer för leverantörsrelationer	
B 6.1	Det ska finnas en vägledning med informationssäkerhetskrav som ska baseras på Norsjö kommuns modell för informationsklassning. Vägledningen ska användas som stöd vid extern upphandling av IT-tjänster
B 6.2	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 finns vägledning, dokumentationsstöd och en kravkatalog i verktyget KLASSA och den kan användas som stöd vid extern upphandling av IT-tjänster såsom system och molntjänster.

KLASSA kan användas som stöd inför användandet av en ny tjänst eller vid kontroll av en befintlig tjänst/leverantör.

Riktlinjer för upphandling av IT-resurser återfinns i avsnitt D7.

Riktlinjer för kontroll av IT-tjänst återfinns i avsnitt C9.

B7 Efterlevnad och granskning

Riktlinjer för efterlevnad och granskning av informationssäkerhet	
B 7.1	Efterlevnaden av informationssäkerhetspolicy och riktlinjerna för informationssäkerhet ska följas upp.
B 7.2	Norsjö kommuns informationssäkerhet bör utsättas för oberoende extern granskning

Efterlevnad av de styrande dokumenten Informationssäkerhetspolicy och detta dokument "Riktlinjer för informationssäkerhet" ska följas upp. I praktiken innebär det främst att riktlinjerna för informationssäkerhet granskas och följs upp; att riktlinjerna efterlevs och att säkerhetsåtgärder införs och får avsedd verkan.

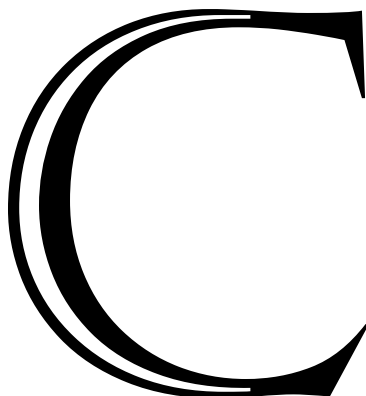
I synnerhet gäller detta de särskilda säkerhetsåtgärder som gäller för information, system och IT-resurser med **höga skydds krav**.

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.

Det är önskvärt att granskning av hela eller stora delar av Norsjö kommuns informationssäkerhet görs regelbundet, genom kommunrevisionen eller av annan granskande part.

Sårbarheter och brister som upptäcks vid granskningar ska tas upp för åtgärdande i genomförandeplaner, handlingsplaner, förvaltningsplaner eller liknande. Akuta sårbarheter och brister ska åtgärdas omedelbart.

Rapportering av större sårbarheter och brister ska ske till ledningsgrupp eller CISO. 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 riktlinjer i Kapitel D – Informationssäkerhet i IT-miljön (avsnitt D10).



Kapitel C Informationssäkerhet i verksamhetsnära förvaltning

Inledning.....	60
Roller och ansvar.....	60
Systemägare.....	60
Systemförvaltare.....	60
Systemadministratör.....	60
Informationsägare.....	60
C 1 Dokumentation av informationssäkerhet.....	61
Systemsäkerhetsbeskrivning.....	61
C 2 Informationsklassning och systemklassning.....	62
C 3 Behörighetshantering och loggning.....	64
Logghantering.....	65
C4 Ändringshantering.....	66
C 5 Användarinstruktioner.....	67
C6 Riskanalys.....	67
C 7 Incidenthantering.....	68
C 8 Kontinuitetshantering.....	69
C 9 Kontroll av IT-tjänst.....	70

Inledning

Kapitel C rör arbetet med informationssäkerhet i verksamhetsnära förvaltning. Kapitlet riktar sig främst till roller i verksamhet och personer som arbetar med informationssäkerhet. I Kapitel D som riktar sig till Norsjö kommuns IT-funktion återfinns informationssäkerhetsrelaterade riktlinjer för den IT-nära förvaltningen. För ett system eller en systemgrupp så ska det finnas en utsedd ägare för det aktuella systemet och som då ansvarar för säkerheten i systemet. De riktlinjer som finns i detta kapitel gäller för dessa.

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 förvaltningsstyrningsmodellen.

Systemägare

I enlighet med Norsjö kommuns informationssäkerhetspolicy är systemägaren ansvarig för informationssäkerhet gällande information i system. Systemägarens motsvarighet i den IT-nära förvaltningen är Ansvarig IT (som bemannas av IT-chef).

Systemägaren ansvarar för att Norsjö kommuns informationssäkerhetspolicy och dessa riktlinjer efterlevs i verksamheten. Systemägaren ska besluta om systemets informationssäkerhetsnivåer genom att klassning sker i enlighet med Norsjö kommuns modell för informationsklassning. Systemägaren ska tilldela tillräckligt med resurser i förvaltningsplaner så att informationssäkerhetsnivån kan uppnås.

Systemförvaltare

Systemförvaltaren leder förvaltningsarbetet och i det ansvaret ingår att system eller grupper av system (s.k. IT-komponenter) klassas så att rätt skyddsnivåer uppnås, och att informationssäkerhetsrelaterade mål och åtgärder nås respektive genomförs. Systemförvaltarens motsvarighet i den IT-nära förvaltningen är Kontaktperson IT.

Systemadministratör

Systemadministratörer ansvarar för att utföra informationssäkerhetsrelaterade aktiviteter på uppdrag av systemförvaltare eller systemägare.

Informationsägare

En informationsägare är den som har ansvar för en viss informationstillgång. Det är nämnd/styrelse som är juridiska informationsägare medan operativa informationsägare är verksamhetens chef. Informationsägaren ska avgöra hur informationen ska klassas och utifrån denna ställa krav på hur information kan och får hanteras och användas. Om ett system har en homogen mängd information som kan [kopplas till den verksamhet som en systemägare ansvarar för, är normalt](#)

systemägaren även informationsägare. I de fall systemägaren inte också är informationsägare för informationen i systemet (till exempel ett diariesystem som hanterar många olika slag av information), så är informationsägare istället kravställare på systemägaren vad gäller säkerheten för den aktuella informationen.

C 1 Dokumentation av informationssäkerhet

Informationssäkerhet i förvaltningsplaner	
C 1.1	Informationsrelaterade mål och åtgärder ska finnas med i systemets förvaltningsplaner

Systemsäkerhetsbeskrivning	
C 1.2	System ska ha en systemsäkerhetsbeskrivning där systemets informationssäkerhet är dokumenterad.
C 1.3	Denna systemsäkerhetsbeskrivning ska gås igenom och vid behov revideras, förslagsvis årligen.

Informationssäkerhet ska vara en naturlig del i förvaltningen av systemet och de IT-komponenter som ingår. Ett system är en IT-komponent. Säkerhetsförhållanden ska vara dokumenterade i systemsäkerhetsbeskrivningar och planerade säkerhetsåtgärder ska ingå i förvaltningsplan så att de formellt fastställs av systemägaren och har en budget. Informationsrelaterade mål och åtgärder ska finnas med i systemets förvaltningsplaner. Mål och åtgärder kan uppkomma eller motiveras med exempelvis resultat från riskanalyser och revisioner, erfarenheter från inträffade incidenter eller krav i dessa riktlinjer.

Systemsäkerhetsbeskrivning

Systemets säkerhetsförhållanden ska dokumenteras i systemsäkerhetsbeskrivningar. En systemsäkerhetsbeskrivning ska finnas för varje system som upphandlas. Gamla system ges systembeskrivning efter hand.

Av systemsäkerhetsbeskrivningen ska det framgå:

- Vilka informationstillgångar som hanteras i systemet och hur dessa är klassade (se avsnitt C2)
- Hur systemet är klassat (se avsnitt C2)

- Hur behörighetshantering och loggning går till (se avsnitt C3)
- Hur ändringshantering går till (se avsnitt C4)
- Användarinstruktioner med inriktning på säkerhet (se avsnitt C5)
- Planerade och genomförda riskanalyser och resultat från dessa (se avsnitt C6)
- Hur incidenthantering går till och vilka incidenter som har inträffat med referenser till incidentrapporter (se avsnitt C7)
- Vilken kontinuitetshantering som finns (se avsnitt C8)

C 2 Informationsklassning och systemklassning

Riktlinjer klassning av system	
C 2.1	Kritiska informationstillgångar i system ska vara inventerad och klassad enligt Norsjö kommuns modell för informationsklassning
C 2.2	System ska klassas som helhet baserat på den klassning som är gjord av kritisk information i systemet
C 2.3	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 skydds krav.

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 Norsjö 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 Norsjö kommuns verksamheter. KLASSA verktyget ska användas som stöd för klassningen.

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 läggs ges den klassning som den ingående informationen har.

Exempel:

Informationstillgång	Konfidentialitet	Riktighet	Tillgänglighet
Information 1	0	3	1
Information 2	1	2	1
Information 3	1	1	2
Systemklassning	1	3	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 skydds krav** för någon informationstillgång i någon aspekt så får systemet automatiskt **höga skydds krav** för denna aspekt. Vid osäkerhet är det bättre att "överklassa" än att "underklassa".

Det viktiga är att kritisk information, dvs. information med **höga skydds krav** 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 skydds krav**.

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 (se avsnitt C5).

C 3 Behörighetshandling och loggning

Riktlinjer för behörighetshandling och loggning	
C 3.1	Det ska finnas dokumenterade processer och/eller rutiner för handtering av behörigheter och rättigheter till system
C 3.2	Varje användare ska ha ett unikt Användar-ID.
C 3.3	Externa användares åtkomst bör vara tidsbegränsad samt föregås av sekretessförbindelse.
C 3.4	Det ska finnas dokumenterade rutiner för logghantering
C 3.5	Höga skydds krav på konfidentialitet, riktighet eller tillgänglighet innebär också höga krav på spårbarhet. Loggning av användares aktiviteter i sådana system är obligatorisk
C 3.6	Förändringar i anställningar och roller ska omedelbart rapporteras av närmaste chef till personalavdelningen så att reglering sker i personal- och lönesystem. Rör förändringen även sådant som IT-enheten administrerar så skickas också meddelande dit.
C 3.7	Uppföljning ska ske av behörighetshandling och logghantering i system.

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 åtkomstilldelning 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, se information under D.2.14).

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 privilegierade användare med särskilda åtkomsträttigheter (administratörer) ska revision ske med kortare intervall. Särskild uppmärksamhet kan behöva ägnas då medarbetare med privilegierade åtkomsträttigheter slutar eller byter tjänst. Sådana processer eller rutiner måste vara kopplade till den IT-nära förvaltningen så att tekniska förändringar genomförs. Ansvarig inom IT (som bemannas av IT-chef) ska säkerställa den del av rutinen som rör införande, förändring samt borttagning av åtkomst i IT-resurser. I Kapitel D finns riktlinjer för hur åtkomstkontroll ska ske i IT-miljön (avsnitt D2 – Styrning av åtkomst). 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. Meddela även IT-avdelningen om förändringen påverkar behörigheter eller tillgång till teknisk utrustning.

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.

C4 Ändringshantering

Riktlinjer för ändringshantering	
C 4.1	Det ska finnas dokumenterade processer eller rutiner för hantering av ändringar i system.
C 4.2	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 en systemändringsprocess eller liknande inom den IT-nära förvaltningen.

I Kapitel D som riktar sig till den IT-nära förvaltningen finns riktlinjer som rör bl.a. systemtest och hantering av testdata (avsnitt D7 – Anskaffning och utveckling av IT-resurser).

Avveckling av system ska ske på ett strukturerat sätt och i samråd med arkivmyndigheten (KS) så att information hanteras i enlighet med den kommungemensamma arkiveringsplanen.

Större förändringar i eller omkring ett system ska föregås av en riskanalys (se avsnitt C6 – Riskanalyser).

C 5 Användarinstruktioner

Riktlinjer för användarinstruktioner	
C 5.1	Informationssäkerhetsregler ska finnas med i användarinstruktioner.
C 5.2	Det ska finnas särskilda instruktioner för hantering av konfidentiell information som t.ex. skyddade personuppgifter (Hög Sekretess (Röd))

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 (se avsnitt C7 – Incidenthantering).
- Eventuell sekretessförbindelse

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

C6 Riskanalys

Riktlinjer för riskanalyser	
C 6.1	Riskanalyser ska genomföras i samband med större förändringar i eller omkring system
C 6.2	Riskanalysresultat ska dokumenteras. Akuta risker ska tas om hand skyndsamt och återstående åtgärder ska tas med i förvaltningsplaner
C 6.3	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 verksamhetens 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 verksamhet, ska en riskanalys genomföras där Norsjö 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.

C 7 Incidenthantering

Riktlinjer för incidenthantering	
C 7.1	Det ska finnas rutiner för hur användare ska rapportera incidenter
C 7.2	Akuta incidenter ska åtgärdas skyndsamt
C 7.3	Allvarliga incidenter ska utredas och dokumenteras.
C 7.4	Avbrottsplaner ska upprättas som innehåller ansvarsförhållanden, kontaktpersoner och eskaleringsvägar.
C 7.5	Samtliga incidenter som rör systemet ska dokumenteras och sammanställas. Kvarstående åtgärdsbehov ska tas om hand i förvaltningsplaner.
C7.6	Personuppgiftsincidenter kopplade till verksamheten ska anmälas till IT-enheten

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 (se C5 – Användarinstruktioner).

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 systemförvaltaren i samverkan med relevanta aktörer, inte minst IT-chef. Om personuppgifter behandlas ska en anmälan om personuppgiftsincident göras. Personuppgiftsincidenten utreds separat men resultatet från systemförvaltarens utredning kan användas som underlag för bedömning av personuppgiftsincidenten, en samordning mellan personuppgiftscoordinator och systemförvaltare kan därför vara lämpligt.

Systemförvaltare 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-nära förvaltningen.

Flera fall av mindre incidenter av likadan art kan tillsammans utmytna 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.

Systemförvaltare ska årligen sammanställa samtliga incidenter som varit kopplade till systemet och som har haft eller kunde ha haft påverkan för verksamhetens informationssäkerhet. Sammanställningen ska redovisas till systemägare, dokumentet är ett viktigt indata till ledningens genomgång för informationssäkerhet.

Kvarstående åtgärdsbehov som inträffade incidenter medfört ska tas om hand i förvaltningsplaner.

C 8 Kontinuitetshantering

Riktlinjer för kontinuitetshantering

C 8.1	Reservplaner och manuella rutiner ska finnas för kritiska system med höga skydds krav gällande tillgänglighet.
C 8.2	Nyckelpersonsberoende ska undvikas och åtgärdas

Krav på kontinuitet av driften av IT-komponenter sker i stora delar genom klassning. Höga skydds krav för tillgänglighet innebär högre krav på säkerhetskopiering och redundans.

Avbrott kan dock ändå alltid ske oavsett vilka förebyggande skyddsåtgärder som finns. Beroendet av funktionalitet i IT-komponenter kan ibland vara så högt att IT-komponenter helt enkelt inte får ligga nere. I dessa fall måste verksamheten ha planer och rutiner för att kunna fullfölja sitt åtagande även vid teknikavbrott.

Nyckelpersonsberoende 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.

C 9 Kontroll av IT-tjänst

Riktlinjer för kontroll av IT-tjänst	
C 9.1	Innan en verksamhetsansvarig börjar använda en IT-tjänst ska den kontrollera att tjänsten kan leverera rätt skydd för verksamhetens information.
C 9.2	Innan en verksamhetsansvarig börjar använda en IT-tjänst ska den ta beslut kring de risker som ett sådant användande kan ge upphov till.
C 9.3	Endast information som är klassad (informationsklassning) får användas i externa IT-tjänster och molntjänster.
C 9.4	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
C 9.5	IT-tjänster som lagrar Känslig Sekretess (Gul) och Hög Sekretess (Röd) information ska kontrolleras minst en gång om året.

Verksamhetsansvarig 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 verksamhetsansvarig 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. Se även B.6.2 om vägledning för kontroll av IT-tjänst.

D

Kapitel D: Informationssäkerhet i IT-miljön

Inledning.....	73
Roller och ansvar	74
IT-säkerhetsansvarig	74
Roller i den IT-nära förvaltningen	75
IT-chef och kontaktperson IT (Systemägare IT och systemförvaltare IT)	75
Ägare av IKT-objekt	75
Systemspecialister IT	75
Incidenthanterare - Incident manager	76
D1 Hantering av tillgångar	76
Identifiering av IT-resurser och tilldelning av ägare	76
Klassning av IT-resurser	77
Användningsinstruktioner.....	77
D2 Styrning av åtkomst	77
Identifiering och autentisering	79
Reglering av åtkomsträttigheter	79
Säkerhetsloggning.....	82
D3 Kryptering.....	83
D4 Fysisk och miljörelaterad säkerhet.....	83

Säkra utrymmen för IT-resurser	85
Godsmottagning och lastning.....	86
Underhåll, reparation och avveckling.....	86
Skydd av utrustning	86
Elförsörjning.....	87
D5 Driftsäkerhet	87
Säkerhetskopiering	88
Loggning och övervakning	90
Hantering av tekniska sårbarheter	91
D6 Kommunikationssäkerhet.....	91
Nätverkssäkerhet.....	92
Informationsöverföring.....	93
D7 Anskaffning och utveckling av IT-resurser	94
Säkerhetskrav på IT-resurser	94
Säkerhetskrav vid upphandling av IT-stöd.....	95
Säkerhet vid systemutveckling	97
Säkerhetskrav vid test	98
D8 Incidenthantering.....	99
Krisorganisation och krisplan.....	101
D9 Kontinuitetsshantering	101
D10 Granskning och kontroll	102

Inledning

Detta kapitel innehåller riktlinjer rörande säkerhet i Norsjö kommuns IT-miljö. Riktlinjerna vänder sig därför främst till chef och medarbetare inom Norsjö kommuns IT-enhet. Riktlinjerna riktar sig också till externa parter som arbetar på uppdrag åt Norsjö 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		Kapitel i 27002
D1	Hantering av tillgångar	Kap 8
D2	Styrning av åtkomst	Kap 9
D3	Kryptering	Kap 10
D4	Fysisk och miljörelaterad säkerhet	Kap 11
D5	Driftsäkerhet	Kap 12
D6	Kommunikationssäkerhet	Kap 13
D7	Anskaffning och utveckling av IT system	Kap 14
D8	Incidenthantering	Kap 16
D9	Kontinuitetshantering	Kap 17
D10	Granskning och kontroll (även B7)	Kap 18

Standarden innehåller mer vägledning och information än vad som finns i dessa riktlinjer, och standarden kan därför användas som ett stödjande dokument för att efterleva riktlinjerna. Inom vissa områden i IT-miljön behöver mer detaljerade instruktioner tas fram som kompletterar eller konkretiserar dessa riktlinjer. Även för detta ändamål kan denna eller andra standarder liksom andra vägledningar, från t.ex. MSB, vara till stöd.

En central del i kommunens informationssäkerhetsarbete är informationsklassning. Information kan ha normala eller höga skydds krav avseende konfidentialitet, riktighet och tillgänglighet i enlighet med klassningsmodell (se Kapitel B).

IT-resurser som hanterar information ska ges ett skydd i enlighet med dessa skyddskrav. Särskilda regler gäller i vissa fall för information som klassats enligt höga skyddskrav i en eller flera av aspekterna konfidentialitet, riktighet och tillgänglighet. Detta markeras genomgående med fetstil och rader i tabeller med riktlinjer har dubbla röda linjer.

Roller och ansvar

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

Ytterst ligger ansvaret på IT-chefen i egenskap av chef för IT-funktionen. Därigenom är IT-chefen ytterst ansvarig för att säkerheten i IT-miljö som tjänster, processer, system, infrastruktur, verktyg etc. är tillräcklig och uppfyller verksamhetens krav, legala krav samt informationssäkerhetspolicyn och dessa riktlinjer för informationssäkerhet.

CISO (chief information security officer)

CISO samordnar arbetet med säkerheten i Norsjö kommuns IT-miljö och är stödjande vid kravställning på externa aktörer.

Ansvar för säkerheten i IT-resurser ligger inte på CISO, 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 riktlinjer och instruktioner för IT-säkerhet,
- stödja verksamheter, systemförvaltning och projekt i IT-säkerhetsfrågor,
- följa upp och granska efterlevnaden av riktlinjer 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 verksamhetens riskanalyser rörande IT-relaterade risker,
- verka för höjande av säkerhetsmedvetande inom IT,
- ta fram statusrapporter för kommunens IT-säkerhet, och

- besvara revisionsrapporter.

CISO arbetar nära kommunens kommunstrateg och interna samverkansgrupper. CISO ska bjudas in till möten som rör informationssäkerhet. CISO ska också omvärldsbevaka, nätverka och samverka externt inom området med exempelvis MSB, cert.se, SIG Security, SKL och andra kommuner.

Roller i den IT-nära förvaltningen

Kapitel C riktar sig till den verksamhetsnära förvaltningen och innehåller informationssäkerhetsrelaterade riktlinjer för denna. I en verksamhet ska det finnas en utsedd ägare för det aktuella systemet och som då har ansvaret för säkerheten i systemet. Det ska finnas utsedda ägare, tekniker osv på IT som kan fungera som motpart till dessa roller så att rätt nivå av säkerhet kan uppnås.

IT-chef och kontaktperson IT (Systemägare IT och systemförvaltare IT)

IT-enheten jobbar för verksamheten med verksamhetens system. Ansvarig inom IT för verksamhetens system kallas ansvarig inom IT (oftast IT-chef). Ansvarig inom IT ansvarar för att IT-säkerheten i IT-komponenter överensstämmer med verksamhetens krav så att rätt säkerhetsnivå upprätthålls och att aktuella IT-komponenter ges ett skydd som motiveras av klassningen av system.

Ansvarig inom IT-enheten (som bemannas av IT-chef) motsvaras i den verksamhetsnära förvaltningen är systemägare verksamhet (som bemannas av verksamhetschef).

IT-chef ansvarar för att Norsjö kommuns informationssäkerhetspolicy och dessa riktlinjer efterlevs inom IT-enheten och ska utse kontaktperson IT för system. Kontaktperson IT samverkar med systemförvaltare verksamhet och i det ansvaret ingår att IT-säkerhetsrelaterade mål och åtgärder i system nås respektive genomförs.

Ägare av IKT-objekt

Det finns en mängd IT-komponenter som inte är system med en ägare i verksamheten. Sådana IT-resurser ingår i IKT-objekt (Informations- och kommunikationsteknik) och kan vara underliggande infrastruktur, stödsystem m.m., och ska ha utpekade ägare som ansvarar för säkerheten i dessa.

Systemspecialister IT

Systemspecialister IT ansvarar för att utföra IT-säkerhetsrelaterade aktiviteter på

uppdrag av ansvarig inom IT, förvaltningsledare IT, ägare av IKT-objekt eller IT-säkerhetsansvarig, eller andra chefer och konsulter.

Incidenthanterare - Incident manager

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

D1 Hantering av tillgångar

Riktlinjer för hantering av tillgångar	
D 1.1	IT-resurser ska identifieras. Den som finansierat IT-resursen är ägare. För IT-resurs utses hos IT-enheten rollerna Ansvarig IT eller IKT-objektägare.
D 1.2	Samtliga IT-komponenter som elektroniskt lagrar och bearbetar information och där information ägs av kommunal myndighet ska förtecknas i systemregistret. Rutiner ska finnas för att hålla förteckningen aktuell och den ska skyddas från åtkomst eller förändring av obehörig.
D 1.3	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.
D 1.4	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. För att föra in rätt skyddsåtgärder för en IT-komponent bör finansiär/ägare se till att komponenten klassas och diskutera skyddsåtgärder tillsammans med IT-enheten. Skyddsåtgärd för IT-komponenten 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.
D 1.5	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 förvaltningsorganisationen, exempelvis verksamhetssystem, har naturliga ägare inom IT i form av ansvariga för IT. Andra IT-komponenter som underliggande infrastruktur, stödsystem m.m., ingår i IKT-objekt och dess ägare är samma som dess finansiär.

Klassning av IT-resurser

IT-komponenter ska klassas i enlighet med Norsjö 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 riktlinjer följas som riktar sig mot IT-miljön och som i vissa fall har särskilda krav för IT-komponenter som hanterar information med höga skydds krav 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

En IT-komponent är en lagrande och bearbetande enhet, dvs en server eller en dator. Det ska finnas regler och instruktioner till hur IT-komponenter får användas. Dessa följer komponenten vid inköp. Om nödvändigt ska nya instruktioner tas fram som baseras på IT-komponenternas klassning och skydds krav 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.

D2 Styrning av åtkomst

Riktlinjer för identifiering och autentisering	
D 2.1	Alla användare ska ha en unik användaridentitet.
D 2.2	Namn på användare, som underlag för t.ex. e-postadresser, ska vara enhetliga i kommunen och stämma överens med namnuppgift i folkbokföringen.

D 2.3	Vid åtkomst till information med höga skyddskrav avseende konfidentialitet eller riktighet ska stark autentisering, i form av tvåfaktorsinloggning, användas.
D 2.4	Stark autentisering bör vara krav vid fjärråtkomst till Norsjö kommuns IT-miljö.
D 2.5	Fjärråtkomst för inloggning med administrativa (priviligierade) konton till IT-resurs med höga skyddskrav avseende konfidentialitet eller riktighet skall vara strikt styrt.
D 2.6	<p>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:</p> <p>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.</p> <p>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.</p> <p>Lösenord får aldrig lagras på ett sätt som gör det möjligt att dekryptera dem till klartext.</p>
D 2.7	För att minska risken för obehörig åtkomst ska samtliga klienter (datorer samt mobila enheter) ska digitalt skärmlås användas 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. I Norsjö har vi strävat mot och har uteslutande teknisk åtkomstkontroll. Det samlade systemet för styrning av åtkomst i en (eller flera) IT-resurs(-er) benämns behörighetskontrollsystem (BKS) och utgörs vanligen av både tekniska system och administrativa rutiner. Detta är ett skallkrav vid nya upphandlingar.

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:

- Ett lösenord eller någonting annat som man vet
- Ett smartkort eller någonting annat som man har
- Ett fingeravtryck eller någon annan egenskap som man är

Stark autentisering är också krav vid extern åtkomst till Norsjö 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

Riktlinjer för reglering av åtkomsträttigheter	
D 2.8	Det ska finnas beslutade och dokumenterade regler och rutiner för behörighetshantering, dvs. BKS, i IT-resurser.
D 2.9	IT-resurser ska ha åtkomsträttigheter som motsvarar hur de är klassade.
D 2.10	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.
D 2.11	Behörigheter till IT-resurser ska vara aktuella och riktiga.
D 2.12	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 planeras för 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.
D 2.13	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 privilegierad åtkomsträtt. Granskning av administrativa rättigheter ska ske löpande med täta intervall.
D 2.14	<p>Gruppidentiteter är inte tillåtna. Eventuella undantag ska godkännas av Systemägare i verksamheten och Ansvarig IT i förening.</p> <p>Gruppidentiteter ska då enbart beviljas under följande förutsättningar:</p> <ul style="list-style-type: none"> • 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
D 2.15	För externa användare gäller att tilldelning av åtkomst, utöver övriga regler för åtkomstilldelning även ska:

	Tidsbegränsas att endast omfatta tiden som behövs för att utföra uppgiften Föregås av sekretessavtal, konsultförbindelse
D 2.16	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 skydds krav avseende konfidentialitet.
D 2.17	Närmaste chef fattar beslut om behörighet till informations-system 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 skydds krav (se ovan).

För verksamhetssystem är det systemägare eller systemförvaltare i verksamheten som beslutar vilka som ska få tillgång till systemet och vilka behörigheter dessa ska ha, samt hur systemet är klassat. Ansvarig IT (som bemannas av IT-chef) 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 behörighetshandlingen, t.ex. att användare får andra arbetsuppgifter eller avslutar sin anställning.

Det kommer att 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 privilegierade användare med särskilda åtkomsträttigheter (administratörer) ska revision ske med kortare intervall. Särskild uppmärksamhet kan

behöva ägnas då medarbetare med privilegierade åtkomsträttigheter slutar eller byter tjänst. Processer och rutiner för behörighetshantering ska följas upp och dokumenteras.

Säkerhetsloggning

Riktlinjer för säkerhetsloggning	
D 2.18	Vid åtkomst till IT-resurs och information med höga skydds krav avseende konfidentialitet eller riktighet krävs loggning av åtkomst för att erhålla spårbarhet.
D 2.19	Loggningsverktyg och logginformation ska skyddas mot manipulation och obehörig åtkomst, logginformation innehållande loggning av åtkomst har alltid höga skydds krav avseende konfidentialitet eller riktighet.
D 2.20	Händelseloggar som registrerar användaraktiviteter, avvikelser, fel och informationssäkerhetshändelser, ska skapas, bevaras en bestämd tid och granskas regelbundet. För loggar som innehåller systemadministratörers aktiviteter gäller att de ska granskas av behörig person 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 informationssäkerhetshändelser. Loggar ska skyddas mot manipulation och obehörig åtkomst, sparas en viss tid och granskas regelbundet av loggadministratör. I de fall logginformation går att knyta till en enskild person är de att betrakta som personuppgifter och omfattas då av krav i 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 personuppgiftsbehandlingen måste hittas, t.ex. samtycke, innan den får ske.

D3 Kryptering

Riktlinjer för kryptering	
D 3.1	Krypteringslösningar ska baseras på etablerade standarder och införande ska godkännas av IT-chef.
D 3.2	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
D 3.3	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 skydds krav på konfidentialitet och/eller riktighet.

Krypteringslösningar ska bygga på etablerade standarder och ska tas fram av Ansvarig IT (som bemannas av IT-chef) i samråd med verksamhetsansvarig och IT-säkerhetsansvarig. Införande av krypteringslösningar ska godkännas av IT-säkerhetsansvarig.

Viktigt att tänka på är att ibland kan krypteringslösningar medföra nya risker relaterade till nyckelhantering.

D4 Fysisk och miljörelaterad säkerhet

Riktlinjer för fysisk och miljörelaterad säkerhet	
D 4.1	Tillträdet till säkra utrymmen ska vara begränsat och regleras minst med hjälp av låssystem med separat nyckelsystem. Nyckel-, kort- och kodinnehav ska vara förtecknade.
D 4.2	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.

D 4.3	Beslut om vem som ges tillträde att arbeta i säkra utrymmen ska vara dokumenterat.
D 4.4	Personal som beviljats tillfälligt tillträde till säkra utrymmen ska i möjligaste mån övervakas under hela besöket.
D 4.5	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
D 4.6	Inkommande gods ska noteras och godkännas av egen personal vid leveranstillfället och eventuella avvikelser från förväntad leverans ska kvitteras av leverantören.
D 4.7	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.
D 4.8	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
D 4.9	Utrymmen som innehåller informationstillgångar med höga skydds krav ska uppfylla Skyddsklass 3 enligt SSF 200 Inbrottskydd.
D 4.10	IT-resurser ska skyddas från elavbrott och andra störningar som orsakas av fel i tekniska försörjningssystem
D 4.11	Synliga kablage för ström och telekommunikation för data eller stödjande informationstjänster ska skyddas från avlyssning, störningar och skada.
D 4.12	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.
D 4.13	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 skydds krav ska sekretessavtal tecknas. Vid känslig information ska informationen döljas, flyttas eller raderas från utrustningen.

D 4.14	Avveckling eller skrotning av IT-resurser och datamedia ska, efter att information som ska bevaras ha förts över till arkivet/arkivmyndigheten (KS), ske genom att information skrivs över, raderas eller förstörs.
D 4.15	Avveckling eller skrotning av datamedia med höga skydds krav 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 eventuellt kommande 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 skydds krav** 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 behörig mottagare 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 skydds krav** 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 försörjningssystem.

D5 Driftsäkerhet

Riktlinjer för drifrutiner	
D 5.1	Det ska finnas formella, beslutade och dokumenterade driftsrutiner för väsentliga processer och system. Dessa ska göras tillgängliga för alla användare som behöver dem. Detta är ett skallkrav i nya upphandlingar.
D 5.2	Ändringar i IT-resurser ska följa fastställd process som säkerställer att ändringarna är riskbedömda, planerade, kommunicerade, testade och godkända.
D 5.3	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

Riktlinjer för skydd mot skadlig kod	
D 5.4	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.
D.5.5	IT-resurser som stöder system med höga skyddskrav ska regelbundet granskas med avseende på skadlig kod.

D 5.6	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.
D 5.7	Det ska finnas en fastställd rutin för återställning av datorer om kommunen skulle drabbas av skadlig kod eller virusutbrott.
D 5.8	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, avsnitt A7 – 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 skydds krav 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 D8 – 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

Riktlinjer för säkerhetskopiering

D 5.9	För IT-resurser med höga skydds krav 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.
-------	--

D 5.10	Baserat på systemets klassning av riktighet och tillgänglighet ska krav definieras för säkerhetskopiering av information.
D 5.11	Det ska finnas en process för återlagring från säkerhetskopior, processen ska vara testad och dokumenterad.
D 5.12	Säkerhetskopiering av information med höga skydds krav 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
D 5.13	Säkerhetskopior ska lagras 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 driftsäkerheten. 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 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 D4 – Fysisk och miljörelaterad säkerhet).

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

Loggning och övervakning

Riktlinjer för loggning och (system)övervakning	
D 5.14	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 systemägares krav.
D 5.15	För att säkerställa all typ av loggning av händelser ska systemklockorna i alla relevanta IT-resurser synkroniseras mot en betrodd referensälla för korrekt tid
D.5.16	Loggningsverktyg och logginformation har höga skydds krav 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. Händeseloggar som registrerar användaraktiviteter, avvikelser, fel och informationssäkerhetshändelser ska skapas, bevaras och granskas regelbundet.

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

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 detta ska därför vidtas.

Hantering av tekniska sårbarheter

Riktlinjer för hantering av tekniska sårbarheter	
D 5.17	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.
D 5.18	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
D 5.19	Säkerhetsgranskning av IT-resurser ska ske, 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.
D 5.20	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 erhålls 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.

D6 Kommunikationssäkerhet

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

Nätverkssäkerhet

Riktlinjer för nätverkssäkerhet	
D 6.1	Krav på skydd vad gäller nätverkstjänster ska identifieras, dokumenteras och tillämpas samt inkluderas i avtal för nätverkstjänster om dessa tjänster tillhandahålls som outsourcade tjänster.
D 6.2	Trådlös datakommunikation innehållande information med normala eller höga skydds krav avseende konfidentialitet är endast tillåtet från godkända klienter. Teknik för att kryptera och säkra kommunikationen ska alltid användas oavsett skydds krav.
D 6.3	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 nätverk efter skyddsbehov. <ul style="list-style-type: none">• Utrustning ska finnas för att kontrollera och förhindra obehörig nätverkstrafik mellan olika nätverkssegment.
D 6.4	Strävan är att brandväggar konfigureras i enlighet med zero-trust modell.
D 6.5	Kommunikationstjänster mellan kommunen och externa nätverk ska dokumenteras och godkännas av IT-chef 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 system, 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

Riktlinjer för informationsöverföring	
D 6.6	Kommunikation med höga skydds krav avseende konfidentialitet och riktighet ska alltid krypteras och kommunicerande parter ska identifieras på ett säkert sätt.
D 6.7	Utgående massutskick av e-post ska begränsas för att förhindra att kapad mailbox används till att skicka ut stora mängder spam.
D 6.8	Överföringslösningar för verksamhetsinformation mellan kommun och externa parter ska regleras genom avtal.
D 6.9	Kommunikation med e-post till andra organisationer skyddas i samtliga epostsystem genom att konfigurera och aktivera standardiserade säkerhetsfunktioner.

Information som hanteras genom elektronisk meddelandehantering ska ges lämpligt skydd. Om meddelande innehållande information med **höga skydds krav** avseende konfidentialitet ska sändas till extern part ska lösning med kryptering och signering användas.

Avtal som reglerar säker överföring av verksamhetsinformation mellan 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 skydds krav avseende konfidentialitet ska överföras.

D7 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

Riktlinjer för säkerhetskrav på IT-resurser

D 7.1	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. Kontakt tas med IT-chef eller annan ansvarig inom IT-enheten som ser till 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 med mera 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

Riktlinjer för säkerhetskrav vid upphandling av IT-stöd	
D 7.2	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.
D 7.3	IT-leverantörer ska på begäran kunna delge hur de bedriver säkerhetsarbete i såväl den operativa verksamheten som avseende säker systemutveckling.
D 7.4	Avtal med IT-leverantör ska innefatta stöd och support i händelse av fel och incidenter.
D 7.5	Avtal med IT-leverantör ska reglera hur kontroll av avtalets uppfyllande ska ske, t.ex. genom tredjepartsrevision eller granskning genomförd av Norsjö kommun
D 7.6	Upphandling av system som ska driftas hos extern leverantör medför ytterligare krav, exempelvis: <ul style="list-style-type: none">• Fördjupade krav på leverantörens interna IT-miljö och informationssäkerhet (t.ex. certifieringar)• Leverantörens kontinuitetshantering• Rätt till tredjepartsrevision• Sekretessavtal• Personuppgiftsbiträdesavtal• Rätt till incidentrapporter från leverantören
D 7.7	Upphandling av IT-stöd ska göras i samverkan med upphandlingsenheten i Arvidsjaur (så länge avtalet gäller med dessa).
D 7.8	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.
D 7.9	Avtal med IT-leverantör ska innefatta: <ul style="list-style-type: none">• Att leverantören innan leverans till Norsjö kommun genomför säkerhetstestning av system och ingående komponenter.• Att testet genomförs av tredje part.

	<ul style="list-style-type: none"> • Att leverantören ska åtgärda eventuella säkerhetsbrister som identifierats i samband med acceptanstest och/eller leveranskontroll.
D 7.10	<p>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:</p> <ul style="list-style-type: none"> • 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 riktlinjer 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 system, 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 kontinuitetsshantering
- 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 upphandlingsregler och fastslagna rutiner för inköp. Till hjälp finns Upphandlingsfunktionen i Arvidsjaur.

Säkerhet vid systemutveckling

Riktlinjer för säkerhetskrav vid systemutveckling	
D 7.11	Processer, rutiner och regler ska finnas som reglerar att informationssäkerhet finns med under hela utvecklingscykeln av IT-resurser
D 7.12	Systemförändringar inom utvecklingscykeln ska styras genom ändringshanteringsprocess, jmf Change managementprocessen.
D 7.13	För systemutvecklings- och integrationsåtgärder ska utvecklingsmiljöer upprättas och skyddas över IT-resursens hela livscykel.
D 7.14	Systemutvecklare ska ha kompetens i programvarusäkerhet.
D 7.15	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

Riktlinjer för säkerhetskrav vid test	
D 7.16	Säkerhetsfunktionalitet ska testas vid utveckling och testning ska göras gentemot de ställda säkerhetskraven och i enlighet med riktlinjer för säker utveckling.
D 7.17	Produktionsdata ska inte användas i test utan all testdata ska väljas ut noggrant, skyddas och styras. Om produktionsdata ändå behöver används gäller följande: <ul style="list-style-type: none">• 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 ansvarig på IT-enheten 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
D 7.18	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.
D 7.19	Driftsättning ska ske enligt fastställd process för ändringshantering avseende berört system (jmf Change management-process).

Säkerhetsfunktionalitet ska testas vid utveckling och testning ska göras gentemot de ställda säkerhetskraven och i enlighet med riktlinjer för säker utveckling. Vid test kan man dra nytta av automatiserade verktyg, 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, jmf Change management-process.

D8 Incidenthantering

Riktlinjer för incidenthantering	
D 8.1	Det ska finnas en incidenthanteringsprocess på IT som omfattar informationssäkerhetsincidenter. Processen ska innefatta: <ul style="list-style-type: none">• 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
D 8.2	Större incidenter ska sammanställas i incidentrapporter som respektive systemägare ansvarar för att ta fram i samverkan med IT.
D 8.3	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
D 8.4	Medarbetare är skyldiga att rapportera informationssäkerhetsincidenter såväl som informations- och IT-relaterade brister i system eller tjänster.
D 8.5	Incidenter där brott eller misstanke om brott föreligger ska alltid polisanmälas och insamling av bevis med mera 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 Norsjö 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-enheten.

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-enheten ska i rollen som "incident manager", incidenthanterare, leda hanteringen av IT-incidenter i samverkan med berörda ägare av systemet. Vid incidenter relaterade till systemet 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 systemägare ansvarar för att ta fram i samverkan med IT-chef. 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

Riktlinjer för krisorganisation och krisplan	
D 8.6	IT-enheten ingår i organisationens krisorganisation för allvarliga incidenter och kriser, som tydligt beskriver roller och ansvar.
D 8.7	Det ska finnas en krisplan som även omfattar IT inom organisationen 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.
D 8.8	Krisplanen ska testas och övas minst en gång per år. Identifierade brister och svagheter ska åtgärdas i syfte att ständigt förbättra krisplanen. 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 (s.k. major incidents) i IT-miljön. Krisplanen ska ha en ansvarig förvaltare och innehålla bland annat krisorganisation, kontaktpersoner och operativa steg att vidta under en allvarlig störning eller kris.

D9 Kontinuitetshantering

Riktlinjer för kontinuitetshantering	
D 9.1	Det ska finnas avbrottsplaner för samtliga kritiska IT-resurser med höga skydds krav avseende tillgänglighet
D 9.2	Övning och testning av avbrottsplaner ska genomföras och utvärderas regelbundet och identifierade brister samt svagheter åtgärdas med syfte att ständigt förbättra kontinuiteten för IT.

D 9.3	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 system med höga skydds krav avseende tillgänglighet måste finnas en beredskap för hur man hanterar avbrott – s.k. avbrottsplaner. IT-chef 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 systemet.

Verksamheten ansvarar för ej IT-mässig, manuell, reservplan för att upprätthålla verksamhet. Avbrottsplaner ska vara relaterade till incidenthanteringen och den övergripande krisplan som ska finnas på IT (se avsnitt D8). En viktig säkerhetsåtgärd för att skapa och bibehålla hög tillgänglighet är säkerhetskopiering (se avsnitt D5).

Målsättningen är att kontinuitetshantering ska utvecklas i hela Norsjö kommun.

D10 Granskning och kontroll

Riktlinjer för granskning och kontroll

D 10.1	Kritiska delar i IT-miljön som stödjer system med höga skydds krav ska regelbundet övervakas och granskas för att sårbarheter och brister ska upptäckas.
D 10.2	Vid osäkerhet gällande säkerhetsförhållanden skall de IT-säkerhetsmässiga förutsättningarna ses över och lyftas till systemförvaltningen.

D 10.3	Sårbarheter och brister som upptäcks vid granskningar ska tas upp för åtgärdande i genomförandeplaner, till exempel förvaltningsplaner. Akuta sårbarheter och brister ska åtgärdas omedelbart
D 10.4	Rapportering av större sårbarheter och brister ska ske till IT-säkerhetsansvarig. IT-säkerhetsansvarig avgör om kommunledningsgruppen behövs informeras.
D 10.5	Revision av hela eller stora delar av IT-miljön ska göras minst vartannat år. Innan granskning eller revision kan ske ska följande beaktas: <ul style="list-style-type: none"> • Behov på åtkomst till system och data inför granskning eller revision ska avtalas med systemägare • 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-säkerhetsansvarig och i förekommande fall till kommunledningsgruppen.

Revision av hela eller delar av IT-miljön ska göras minst vartannat år. Revision eller mätning av kommunens informationssäkerhet i stort kan även omfatta IT- miljö.

Index – hänvisning till riktlinjetabeller

Användarinstruktioner ska finnas (C5)	67
Autentisering (D2)	77
Behörighetshantering (C3)	64
Dokument om informationssäkerhet – struktur (B2)	47
Drifrutiner för väsentliga processer och system (D5)	87
Etiska riktlinjer (A8)	33
Identifiering (D2).....	77
Incidenthantering (C7).....	68
Incidenthantering (D8)	99
Information – muntlig (A10).....	37
Information - på skärmar och papper (A10).....	38
Informationssäkerhet - efterlevnad och granskning (B7).....	57
Internetanvändning (A8)	32
IT-miljö - granskning och kontroll (D10)	102
IT-tillgångar – hantering (D1).....	76
Klassificering – Information (B3)	49
Klassificering – system (C2)	62
Kontinuitetshantering (C8)	69
Kontinuitetshantering (D9).....	101
Krisorganisation och krisplan (D8).....	101
Kryptering (D3)	83
Lagring – Användarriktlinjer (A5).....	25
Lagring - G Drive, utb (A5)	27
Lagring – molntjänster (A5)	26
Lagring - Onedrive/SharePoint (A5).....	27
Leverantörsrelationer (B6)	57
LIS - Ledningssystem för informationssäkerhet (B4)	53
Loggning – fördjupad granskning (A9).....	35
Loggning - Gallring av granskningsloggar (A9).....	35
Loggning - Granskning av loggar (A9)	34
Loggning – Loggning i IT-resurs och systemövervakning (D5).....	90
Loggning – Säkerhetsloggning (D2)	82
Loggning - övervakning av användaraktiviteter etc (C3).....	64
Lösenord – hantering (A2).....	22
Lösenord – utformning (A2)	21
Mobila enheter – hantering (A6).....	28
Mobila enheter - Smarta telefoner/surfplattor, särskilda regler	30
Nätverkssäkerhet (D6).....	92
Personalsäkerhet - före och i samband med anställning (B5).....	54
Personalsäkerhet - under anställning (B5)	54
Personalsäkerhet - vid avslut eller ändring av anställning (B5).....	55
Risker – analys och hantering (C6)	67
Skadlig kod – skydd mot (A7).....	31
Skadlig kod - skydd mot (D5)	87

Sociala medier – användning (A8)	34
Systemutveckling – säkerhetskrav (D7).....	97
Säkerhet – Fysisk och miljörelaterad (D4)	83
Säkerhetskopiering – IT-enheten (D5).....	88
Säkerhetskopiering (A5)	25
Säkerhetskrav på nya IT-resurser (D7).....	94
Tekniska sårbarheter – hantering (D5).....	91
Tester – säkerhetskrav (D7)	98
Upphandling av IT-stöd - säkerhetskrav (D7)	95
Verksamhetens kontroll av IT-tjänst – inför användning och löpande (C9).....	70
Åtkomsträttigheter – reglering (D2)	79
Ändring gällande system (C4)	66
Överföring av verksamhetens information (D6).....	93

Bokstav inom parentes motsvarar kapitel...

Kapitel A: Informationssäkerhet för medarbetare

Kapitel B: Styrning av informationssäkerhet

Kapitel C: Informationssäkerhet i verksamhetsnära förvaltning

Kapitel D: Informationssäkerhet i IT-miljön

