

Riktlinjer för informationssäkerhet

Örebro kommun



PROGRAM

Uttrycker värdegrund och önskvärd utveckling av verksamheten.

POLICY

Uttrycker ett värdegrundsbaserat förhållningssätt och principer för vägledning.

STRATEGI

Konkretiserar ett program eller en policy och utgör en grund för Prioritering.

HANDLINGSPLAN

Beskriver konkreta mål och åtgärder.

RIKTLINJER

Säkerställer ett riktigt agerande och en god kvalitet vid handläggning och utförande.

Beslutad av Kommundirektören, den 23 april 2025

Dokumentansvarig på politisk nivå: Kommunstyrelsen

Dokumentansvarig på tjänstemannanivå: Kommundirektören

Informationsklass: Intern

Innehåll

Inledning	5
Riktlinjernas omfattning	5
Struktur och läsanvisningar	5
Dispenser och avsteg	6
Introduktion till informationssäkerhet	6
Relevanta termer och definitioner	8
Kapitel A: Informationssäkerhet för medarbetare	9
Inledning	11
Medarbetarens ansvar för informationssäkerhet	11
Informationsklasser	12
A1. Lösenord	14
A2. Mobila enheter	15
A3. Skadlig kod	16
A4. Internet och sociala medier	17
A5. Digital kommunikation	18
A6. Lagring och säkerhetskopiering	19
A7. Spårbarhet och loggning	20
A8. Säkert beteende	20
Kapitel B: Styrning av informationssäkerhet	22
Inledning	24
B1. Roller, ansvar och organisation	24
B2. Dokumentstruktur	26
B3. Informationsklassning	27
B4. Ledningssystem för informationssäkerhet	30
B5. Personalsäkerhet	31
B6. Leverantörsrelationer	32
B7. Efterlevnad och granskning	33
Kapitel C: Informationssäkerhet i verksamhetsnära förvaltning	34
Inledning	36
Roller och ansvar	36
C1. Dokumentation av informationssäkerhet	37
C2. Informationsklassning och systemklassning	37
C3. Behörigheter och logghantering	39
C4. Ändringshantering	40
C5. Användarinstruktioner	41
C6. Riskanalyser	41
C7. Incidenthantering	42
C8. Kontinuitetshantering	42
C9. Kontroll av IT-tjänst	43
Kapitel D: Informationssäkerhet i IT-miljön	44
Inledning	46
Roller och Ansvar	46

D1.	Hantering av tillgångar	47
D2.	Styrning av åtkomst	49
D3.	Kryptering.....	52
D4.	Fysisk och miljörelaterad säkerhet	53
D5.	Driftsäkerhet.....	56
D6.	Kommunikationssäkerhet.....	60
D7.	Anskaffning och utveckling av IT-resurser	62
D8.	Informationssäkerhetsincidenter	65
D9.	IT-relaterad kontinuitetshantering	67
D10.	Granskning och kontroll.....	68
Figur 1:	Informationssäkerhetens tre aspekter	7
Figur 2:	I Örebro kommun används tre informationsklasser.	12
Figur 3:	Dokument för styrning av informationssäkerhet.....	27
Figur 4:	Örebro kommuns modell för informationsklassning.....	28

Inledning

Örebro kommuns informationshanteringspolicy är ett övergripande dokument som redovisar kommunens övergripande mål och inriktning med informationshantering. Detta dokument – Riktlinjer för informationssäkerhet – konkretiserar informationshanteringspolicyen med mer detaljerad information och regler för hur information ska hanteras inom kommunen.

Dessa riktlinjer är fastställda av kommundirektören och gäller från och med 2025-04-23.

Riktlinjernas omfattning

Dessa riktlinjer innehåller information och riktlinjer gällande säkerhet vid all hantering av information inom Örebro kommun.

Riktlinjerna gäller för alla verksamheter i Örebro kommun, vilket medför att det inte finns utrymme att besluta om lokala riktlinjer eller rutiner som avviker från dessa.

Riktlinjerna gäller inte för kommunens bolag, utan dessa beslutar om 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 när det finns särskilda behov av samordning.

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	Sidor
A	Informationssäkerhet för medarbetare	Information och riktlinjer för hur information och IT ska hanteras i olika situationer.	Alla medarbetare 9-21
B	Styrning av informationssäkerhet	Ansvarsfördelning för informationssäkerhet. Information och riktlinjer för hur arbetet med informationssäkerhet ska bedrivas.	Alla som arbetar med IT- och informationssäkerhet 22-33
C	Informationssäkerhet i verksamhetsnära förvaltning	Information och riktlinjer för informationssäkerhet i förvaltningsobjekt som t.ex. system och grupper av system.	Informationsägare, objektägare och förvaltningsledare 34-43
D	Informationssäkerhet i IT-miljön	Information och riktlinjer för hur information och IT ska hanteras inom IT-miljön, dvs. IT-säkerhet.	Chefer och medarbetare på digitaliseringsavdelningen 44-68

Varje kapitel består både av informativa avsnitt och av riktlinjer som är obligatoriska. Samtliga riktlinjer är numrerade och i tabellform med rött huvud. Rader som innehåller riktlinjer för **konfidentiell** information och **höga skydds krav** har dubbla linjer och nämnda termer är dessutom fetmarkerade. Exempel från Kapitel A om lagring i molntjänster:

Riktlinjer för lagring i molntjänster	
A.6.8	Endast godkända molntjänster är tillåtna att användas. Kontrollera vilka molntjänster som är tillåtna inom din verksamhet.
A.6.9	Konfidentiell information får inte lagras i personliga molntjänster.

Andra tabeller, som inte innehåller riktlinjer, har tabellhuvuden i lila 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. Örebro 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 tidigare versioner av Örebro kommuns riktlinjer för informationssäkerhet är denna baserad på den svenska och internationella standardserien SS-ISO/IEC 27000.

Dispenser och avsteg

Ansökan om avsteg från dessa riktlinjer ska ställas till kommunens informationssäkerhetsråd. Sådana ärenden ska beredas innan de ställs till rådet för att underlätta beslut. Exempelvis kan en riskanalys ingå i beredningen av ärendet. Beslut om godkännande av avsteg ska fattas av kommunens informationssäkerhetsansvarige i samråd med berörda.

Avsteg från Riktlinjer för informationssäkerhet får aldrig vara permanenta utan ska ha en giltighetstid på som längst 1 år. Om behov av avsteg kvarstår ska ärendet beredas på nytt och nytt beslut fattas om eventuellt godkännande.

Introduktion till informationssäkerhet

Information finns i alla kommunens verksamheter och handlar om allt det vi gör, exempelvis om vår personal, våra tjänster, vår ekonomi och det omgivande samhället med medborgare, företag, föreningar osv. Information är därför i sig en av kommunens viktigaste tillgångar.

Den ökade graden av digitalisering medför mycket möjligheter för Örebro kommun som organisation, men även utmaningar och hot. Information är inte längre enbart organisationsinterna tillgångar och angelägenheter, utan kan flöda mellan organisationer i näringsliv och offentlig förvaltning, till och mellan enskilda, och över nationsgränser. Linjer suddas ut mellan vem som "äger" och bär ansvar för information, och det blir svårare att definiera hur den får och kan användas, samt var ursprungsinformationen finns osv.

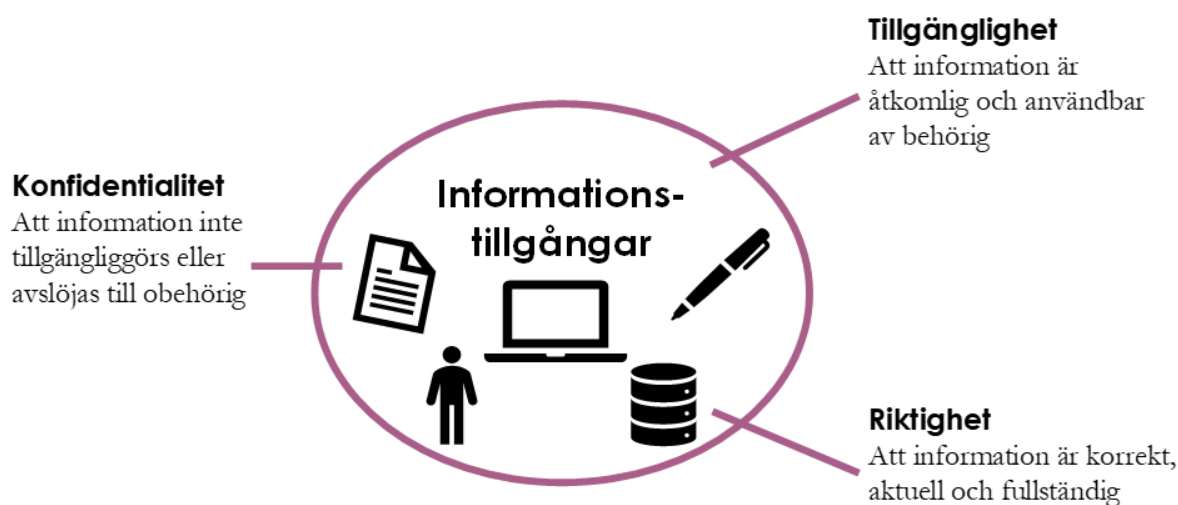
Utveckling där informationshantering och informationsflöden antar nya former i samhället, i kombination med en ökad och förändrad hotbild, innebär att informationssäkerhet är en förutsättning för att Örebro kommun kan delta i det digitala samhället. Det sker mängder av informationsrelaterade incidenter i Sverige och internationellt som beror på avsiktliga attacker såväl som misstag och olyckor. En god informationssäkerhet möjliggör därför säker och tillförlitlig användning av ny teknik och är en nödvändighet för digitalisering.

Informationssäkerhet handlar om att skapa och upprätthålla lämpligt skydd av informationen. Detta innefattar information i alla dess former; text, ljud, bild, film, tal osv, och oavsett hur

den lagras, bearbetas och kommuniceras. Till skillnad från IT-säkerhet, som fokuserar på säkerheten i IT-baserad informationshantering, så omfattar alltså informationssäkerhet *all* information, oavsett *hur* eller *var* informationen hanteras.

Informationssäkerhet har inget egenvärde, utan ska bidra till att Örebro kommun når sina övergripande visioner, strategier och mål. Örebro kommun ska uppnå och upprätthålla en informationssäkerhet som uppfyller mål i övergripande policys och strategidokument.

Information och de resurser som används för att hantera information benämns informationstillgångar. Informationssäkerhet utgår från tre aspekter; konfidentialitet, riktighet och tillgänglighet (se Figur 1).



Figur 1: Informationssäkerhetens tre aspekter

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 t.ex. stjälas, raderas, förändras eller göras otillgänglig.

En viss informationsmängd har krav på sig gällande de tre aspekterna. Kraven kan vara interna eller härledas från rättsliga krav, förväntningar eller behov från externa aktörer. Lagar, förordningar, föreskrifter och avtal ställer rättsliga krav på en verksamhets informationshantering som ofta inbegriper krav på informationens konfidentialitet, riktighet och tillgänglighet. Dessutom har externa aktörer ofta behov och förväntningar som påverkar organisationens informationssäkerhet.

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

Relevanta termer och definitioner

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	Representation av fakta i form av t.ex. tecken eller signaler som är lämpad för överföring, tolkning eller bearbetning av människor eller av automatiska hjälpmedel.
Information	Innebörd i data, d.v.s. data tolkad av människor.
Informationsklassning	Att genom konsekvensanalys identifiera skyddsbehovet för en viss informationsmängd.
Informationssäkerhet	Konfidentialitet, riktighet och tillgänglighet hos information.
Informationshanteringspolicy	Kommunens viljeinriktning med informationssäkerhet uttryckt av vår ledning.
Informationstillgång	Information som är av värde för organisationen, och även de resurser som hanterar den, exempelvis människor, papper, mjukvara, hårdvara och immateriella tillgångar (t.ex. rykte).
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 administrativt ledningssystem som syftar till att upprätta, införa, driva, övervaka, granska, underhålla och förbättra organisationens informationssäkerhet.
Riktighet	Att information är korrekt, aktuell och fullständig.
Sekretess	Sekretess innebär att viss information skyddas och inte får spridas till obehöriga. Det kan gälla personuppgifter, intern information eller annan känslig information som skyddas för att förhindra skada eller missbruk.
Spårbarhet	Entydig härledning av utförda aktiviteter till en identifierad användare eller IT-resurs.
Tillgänglighet	Att information är åtkomlig och användbar av behörig.



Kapitel A: Informationssäkerhet för medarbetare

Innehåll Kapitel A

Kapitel A: Informationssäkerhet för medarbetare	9
Inledning	11
Medarbetarens ansvar för informationssäkerhet.....	11
Informationsklasser.....	12
A1. Lösenord	14
A2. Mobila enheter	15
A3. Skadlig kod	16
A4. Internet och sociala medier	17
A5. Digital kommunikation	18
A6. Lagring och säkerhetskopiering	19
A7. Spårbarhet och loggning	20
A8. Säkert beteende	20

Inledning

Detta kapitel vänder sig till alla medarbetare vid Örebro kommun. Riktlinjerna gäller även externa användare som har åtkomst till Örebro kommuns information.

Riktlinjerna beskriver det ansvar man som medarbetare har vid hantering av information i Örebro kommun och vilka regler som gäller.

Örebro kommun är en stor organisation med många skilda verksamheter. Kompletterande regler till riktlinjerna kan därför finnas lokalt. Avvikelser från dessa riktlinjer får dock aldrig göras utan särskilt tillstånd. Kontakta ansvarig chef vid osäkerhet om vad som gäller.

På denna sida finns information om arbetet med informationssäkerhet i Örebro kommun samlad: <http://intranat.orebro.se/informationssakerhet>

Medarbetarens ansvar för informationssäkerhet

Information är en viktig resurs för Örebro 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 t.ex. för- och grundskola, gymnasium, socialtjänst, hemvård, stadsplanering, bygglov etc. 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. Det finns lagar och föreskrifter som kommunen måste leva upp till. Dessutom har privatpersoner, företag och andra 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 typer 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 m.m. Även medarbetares kunskap och medvetenhet är ett viktigt skydd, t.ex. hur vi arbetar i IT-system och med pappersdokument. 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 Örebro kommuns informationssäkerhet beror därför på hur den enskilde medarbetaren hanterar informationen.

Örebro kommun ställer krav på att medarbetare följer dessa riktlinjer för informationssäkerhet. Chefer har ett ansvar att delge information och utbildning i informationssäkerhetsfrågor till sina medarbetare.

Om du som medarbetare eller externt kontrakterad har tillgång till känslig information ska du vara medveten om tystnadsplikt och sekretess. Detta gäller även efter att anställningen upphört.

Vid underlåtenhet att följa dessa riktlinjer för informationssäkerhet följer Örebro kommun de lagar och avtal som reglerar vår verksamhet. Brottsliga aktiviteter polisanmäls.

Skyldighet att rapportera incidenter och brister

Alla medarbetare har skyldighet att rapportera incidenter eller brister som misstänks kunna medföra negativ påverkan på Örebro kommun. När det gäller informationssäkerhet kan det till exempel röra sig om till exempel:

- IT-angrepp/intrång
- Skadlig kod
- Oskyddad känslig information
- Brister i efterlevnad av dessa riktlinjer för informationssäkerhet
- Social manipulation för att kringgå säkerheten

Incidenter och brister ska rapporteras till Kommunsupport (20 00). 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.

Informationsklasser

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

I Örebro kommun finns tre klasser för hur känslig informationen är och hur den får spridas: Öppen, Intern eller Konfidentiell¹. Dessa illustreras i Figur 2.

Informationsklass	Behörighet/spridning	Exempel
2 Konfidentiell information	Konfidentiell information får endast vara tillgänglig för medarbetare som har särskild behörighet att hantera informationen.	<ul style="list-style-type: none"> • Känsliga personuppgifter • Patientjournaler • Sekretessbelagd information
1 Intern information	Intern information ska endast spridas till medarbetare inom Örebro kommun och till externa som har behov av informationen.	<ul style="list-style-type: none"> • Riktlinjer • Instruktioner • Information på intranät
0 Öppen information	Öppen information kan spridas fritt inom och utom Örebro kommun.	<ul style="list-style-type: none"> • Pressmeddelanden • Broschyrer • Information på www.orebro.se

Figur 2: I Örebro kommun används tre informationsklasser.

¹ Figur 4: Örebro kommuns modell för informationsklassning beskrivs i Kapitel B – Styrning av informationssäkerhet innehåller förutom konfidentialitet även aspekterna riktighet och tillgänglighet.

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

- Öppen information har inga krav på åtkomstbegränsning utan kan spridas fritt. Ibland krävs dock beslut för att öppen information ska publiceras, t.ex. på extern webbplats som www.orebro.se.
- För Intern information gäller de normala hanteringsregler som finns nedan i avsnitt A1 – A8. Intern information kan normalt spridas internt inom kommunen. Om intern information sprids till extern aktör ska det finnas ett tydligt syfte med detta.
- Särskilda hanteringsregler gäller för **konfidentiell** information. I detta kapitel är all information och alla riktlinjer som gäller för **konfidentiell** information markerad med fetstil och med dubbla ramar i tabeller med riktlinjer.

Det är viktigt att **konfidentiell** information hanteras på rätt sätt. **Konfidentiell** information är bl.a. känsliga personuppgifter och sekretessklassad information.

Örebro kommuns samtliga verksamheter hanterar personuppgifter av olika slag. Personuppgifterna ska behandlas i enlighet med gällande författningar, såsom exempelvis dataskyddsförordningen, dataskyddslagen och lagen om behandling av personuppgifter inom socialtjänsten. Personuppgifter kan vara klassade som **konfidentiell**, intern eller öppen information. Det beror på sammanhanget, samt vilka personuppgifter som avses.

Skyddade personuppgifter är alltid **konfidentiell** information och ska hanteras utifrån särskilda rutiner och regler. Med skyddade personuppgifter avses skyddad folkbokföring, sekretessmarkering samt fingerade uppgifter (vilket innebär att man har fått nytt namn och personnummer).

➔ **Se vidare i Riktlinjer för dataskydd.**

Örebro kommun som offentlig organisation hanterar allmänna handlingar enligt offentlighet- och sekretesslagen (2009:400). När en allmän handling begärs ut ska Örebro kommun alltid genomföra en sekretessprövning med stöd i offentlighet- och sekretesslagen eller annan tillämplig lagstiftning. Endast den information som inte omfattas av sekretess kan lämnas ut. Sekretessbelagd information klassas alltid som **konfidentiell**.

Arbetsmaterial som tas fram under ett ärendes beredning, anteckningar, verksamhetsinterna meddelanden och personliga meddelanden är som huvudregel inte allmänna handlingar. Däremot innehåller dessa typer av handlingar information som ska klassas som **konfidentiell**, intern eller öppen beroende på innehållet.

➔ **Se vidare i Riktlinje för hantering av allmänna handlingar.**

A1. Lösenord

Användar-ID och lösenord används för att skydda Örebro kommuns information och det är därför viktigt att följa nedanstående regler för utformning och hantering av lösenord.

För att förhindra att någon obehörig kan få tillgång till din information och dina användarkonton så är det avgörande att skydda dina lösenord. Om en obehörig person får tillgång till både ditt användar-ID och lösenord så kan den personen utföra aktiviteter i ditt namn. Lösenorden är därför personliga och får inte delas eller göras kända för andra.

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.

Riktlinjer för utformning av lösenord	
A.1.1	Lösenord ska vara minst 14 tecken långt.
A.1.2	Lösenord ska innehålla minst en siffra, en versal (ej å, ä eller ö) och ett specialtecken (t.ex. ! % & #)

Via Örebro kommuns lösenordsportal blir du påmind om när lösenord behöver bytas och kan få ett nytt om du har glömt ditt lösenord. För att komma ihåg ditt lösenord är ett tips att formulera det utifrån en mening.

Exempel:

”Klockan 10 går ett tåg till Norrköping med ett byte i Hallsberg!”

“Jag har en ärta i näsan, pilutta dej, det har inte du!”

Lösenord:

K10g1ttNmebiH!

jH1ainPddHidu!

Användar-ID är intern information och lösenord är **konfidentiell** information och ska därför hanteras på ett säkert sätt:

Riktlinjer för hantering av lösenord	
A.1.3	Lösenord ska inte vara synliga. Lösenordet ska hanteras som en värdehandling och inte ligga framme uppskriven på en lapp. Bäst är att förvara lösenord endast i minnet.
A.1.4	Olika lösenord ska användas. Samma lösenord ska inte användas privat och i jobbet. Olika lösenord ska dessutom användas för olika tjänster på webben även om de är jobbrelaterade. Om tjänsten erbjuder möjligheten till att använda multifaktorsautentisering, bör du använda det.
A.1.5	Lösenord ska bytas regelbundet. Lösenordsportalen tvingar fram byte av lösenord var 180:e dag. I system där lösenordsbyte inte är tvingande, ska lösenordet ändå bytas några gånger om året. Vid misstanke om att lösenord har röjts ska byte ske omedelbart.
A.1.6	Lösenord får inte delas. Lösenord är personliga och ska inte delas mellan kollegor. Man kan i så fall bli anklagad 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.1.7	Automatisk minnesfunktion för lösenordet ska inte användas. Om man loggar in på webbsidor så ska man inte låta webbläsare spara lösenordet, utan alternativet ”Nej” ska väljas om man får en sådan fråga. Detta är särskilt viktigt då en dator delas av flera. 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.

A2. Mobila enheter

Den IT-utrustning som tillhandahålls av Örebro kommun kan vara stationär eller bärbar, en s.k. mobil enhet. Med mobil enhet avses bärbar dator (laptop), smart telefon (mobiltelefon), surfplatta, samt USB-minne, CD/DVD-skiva, extern hårddisk.

Applikationsspecifika datorer, smarta telefoner eller surfplattor som exempelvis TES-mobiler, kan ha specifika riktlinjer utöver dessa som presenteras här.

Riktlinjer för hantering av mobila enheter	
A.2.1	Mobila enheter som tillhandahålls av Örebro kommun är arbetsredskap och får inte lånas ut eller överlåtas, om det inte är enheter som delas av flera.
A.2.2	Uppsatta säkerhetsinställningar i enheter får inte ändras.
A.2.3	Endast av Örebro kommun godkända programvaror får installeras på enheten.
A.2.4	Installerad programvara får inte kopieras eller installeras på annan enhet.
A.2.5	Mobila enheter ska låsas med lösenord, om funktion för lösenord finns.
A.2.6	Konfidentiell information måste vara krypterad på mobila enheter.
A.2.7	Viktig information bör inte lagras enbart på en enhet, i så fall ska den snarast kopieras över till kommunens nätverk så att informationen säkerhetskopieras.
A.2.8	Endast av kommunen godkänd enhet och programvara får anslutas till kommunens nät.
A.2.9	Privat utrustning kan anslutas till kommunens gästnät. Vissa verksamheter har dessutom ett trådlöst nätverk för privata enheter som datorer, smarta telefoner och surfplattor (s k Bring Your Own Device – BYOD).
A.2.10	Enheten får enbart anslutas till trådlösa nätverk som är kända och lösenordskyddade.
A.2.11	Vid distansarbete måste godkänd säker utrustning och anslutning användas.
A.2.12	Anslutning med kommunens VPN-anslutning från en privat dator är ej tillåtet.

Riktlinjer för fysisk hantering av mobila enheter	
A.2.13	Försiktighet ska iakttas vid arbete i publika miljöer, exempelvis kan skärmen skyddas med sekretesskydd.
A.2.14	Arbete med konfidentiell information får inte ske i publika miljöer.
A.2.15	Mobila enheter får inte lämnas utan uppsikt och ska förvaras i säkert utrymme.
A.2.16	Förlust av enhet ska omedelbart anmälas till Kommunsupport, detta ska göras innan polisanmälan. I vissa fall finns möjligheter att fjärradera information för att begränsa skadans omfattning.
A.2.17	Mobil enhet får inte behållas privat efter avslutad anställning eller vid byte till ny/annan mobil enhet. Mobil enhet med tillbehör ska återlämnas till Örebro kommun.
A.2.18	Utrustningen ska i övrigt vårdas och hanteras på det sätt som föreskrivs, t.ex. skyddas mot värme och fukt med skärmskydd och skal.

Förutom de riktlinjer som gäller allmänt för mobila enheter gäller även följande vid användning av smarta telefoner och surfplattor:

Riktlinjer för smarta telefoner och surfplattor	
A.2.18	Örebro kommun är som arbetsgivare ägare till de smarta telefoner och surfplattor som används i tjänsten och även till den information som finns i dessa. Man bör därför som medarbetare vara medveten om att arbetsgivaren har rätt att ta del av t.ex. sms, foton och kalenderanteckningar. Eftersom offentlighetsprincipen gäller kan utomstående begära ut informationen.
A.2.19	Det är endast tillåtet att ladda ned appar från företagsportalen för iOS, App Store och Google Play för Android. Genom att ladda ner från dessa betrodda källor minskar risken att ladda ner appar med skadlig kod.
A.2.20	Konfidentiell information får inte hanteras i smart telefon eller surfplatta om inte särskild av kommunen godkänd säkerhetslösning används.
A.2.21	Pinkoder, fingeravtryck eller annan autentisering måste användas till smarta telefoner och surfplattor. Då pinkoder används ska ej enkla pinkoder som 0000, 1234 etc. användas, och inte samma pinkod som används i andra sammanhang, t.ex. pinkod till bankomatkort.

A3. Skadlig kod

Skadlig kod är ett samlingsbegrepp för oönskade datorprogram som virus, trojaner, spionprogram och maskar. Skadlig kod kan installeras på en dator eller ett nätverk utan administratörens samtycke och har utvecklats i syfte att störa IT-system, samla in information eller för att utnyttja datorkraft i IT-utrustning.

Skadlig kod är ett växande problem och blir alltmer sofistikerad och ”intelligent” och kan vara svår att upptäcka. Idag behöver man inte vara tekniskt kunnig för att själv skapa skadlig kod, utan det kan enkelt köpas på marknadsplatser på Internet.

Exempel på idag förekommande skadlig kod:

- Trojaner som kan avlyssna lösenord och skicka dessa vidare, så kallade ”keyloggers”.
- Trojaner som skapar bakhåll i datorer så att andra personer får tillgång till dess innehåll utan ägarens vetskap.
- Ransomware där filer eller diskar på dator, smart mobil eller surfplatta krypteras och där en lösensumma krävs för att få tillbaka åtkomst till filerna.

Spridning av skadlig kod

Skadlig kod kan spridas till dator eller mobila enheter t.ex. genom att öppna bilagor i e-post, importera filer eller surfa på Internet och klicka på infekterade länkar. Infekterade länkar kan även finnas i sociala medier.

Det bästa skyddet mot skadlig kod är att vara medveten om hot och bedöma rimligheten i det som händer på din skärm. Avsändare av e-post kan förfalskas och webbsidor är inte alltid det som de utger sig för att vara. Konton på sociala medier kan kapas och falska e-postadresser kan skapas i syfte att lura mottagaren till att klicka på länkar. Vid så kallade ”Phishing” luras mottagaren att klicka på en länk som leder till en sida där man ombeds fylla i koder, lösenord eller bankkontouppgifter. Var observant på detta och fyll aldrig i denna typ av uppgifter. Seriösa företag, organisationer och myndigheter ber inte om uppgifter på detta sätt.

Skadlig kod kan spridas och orsaka stor skada om smittad IT-utrustning kopplas upp mot kommunens nätverk, även via till exempel ett smittat USB-minne.

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:

Riktlinjer för skydd mot skadlig kod	
A.3.1	Stäng aldrig av eller på annat sätt inaktivera installerat skydd mot skadlig kod.
A.3.2	Anslut endast godkänd IT-utrustning till kommunens nätverk.
A.3.3	Var misstänksam och undvik att klicka på konstiga länkar eller fyll i irrelevanta uppgifter.
A.3.4	Öppna bifogade filer endast om de kommer från en känd avsändare och en bilaga är förväntad.
A.3.5	Var observant på om IT-utrustning betar sig långsamt eller konstigt. Vid misstanke om skadlig kod kontakta Kommunsupporten.

A4. Internet och sociala medier

Förutom de riktlinjer som är kopplade till skadlig kod i avsnitt A3 finns här särskilda regler för användning av Internet och sociala medier.

Riktlinjer för Internetanvändning	
A.4.1	Internet är i arbetet på Örebro kommun främst ett arbetsverktyg och ska inte störa ordinarie arbetsuppgifter eller innebära merkostnader för kommunen.
A.4.2	De lagar som gäller i samhället i övrigt gäller självklart även vid användning av internet inom Örebro kommun. Tryckfrihetsförordningen, offentlighet- och sekretesslagen, dataskyddsförordningen, brottsbalken och lagen om upphovsrätt är exempel på sådana lagar.
A.4.3	För material på Internet som ska användas i tjänsten, får nedladdning och installation av upphovsrättsligt material (datorprogram, film, musik, m.m.) inte ske utan stöd i lag, avtal eller med skriftligt tillstånd från rättighetsinnehavaren.
A.4.4	I begränsad omfattning får internet användas för privata syften. Utrymmeskrävande filtyper inklusive filmer, program och spel får dock inte för privat bruk laddas ned, strömmas, lagras eller spridas i, eller via, Örebro kommuns nätverk.
A.4.5	Internet är ett öppet nätverk och endast öppen information får publiceras eller delas, alltså inte intern eller konfidentiell information.

Uttalanden och andra aktiviteter som görs på Internet och sociala medier kan påverka allmänhetens uppfattning om den enskilde tjänstemannen som utför aktiviteten, samt för Örebro kommun. Det finns dessutom en risk att ett engagemang i tvivelaktiga sammanhang kan öka risken för att bli en måltavla för social manipulation. Det är därför viktigt att som representant för Örebro kommun beakta god etik och gott omdöme på internet. Örebro kommuns etiska regler och värderingar ska följas även vid kommunikation via internet och sociala medier. Tänk därför på att:

Etiska riktlinjer	
A.4.6	All kommunikation på Internet från konton som tillhör Örebro kommun ska vara öppen, saklig och etisk, oavsett om kommunikationen sker för privata syften eller inte.

A.4.7	Det är inte tillåtet att besöka webbplatser med till exempel brottslig verksamhet, rasism, diskriminering, extrempolitiskt eller pornografiskt innehåll.
A.4.8	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 nog innan du publicerar.

Örebro kommun är aktivt på sociala medier. Den personal som skriver i Örebro kommuns namn har särskilda regler och kunskap om kommunikation.

→ Se vidare i Riktlinjer för sociala medier i Örebro kommun.

A5. Digital kommunikation

Det finns många typer av digital kommunikation som via skrift, bild och ljud kan skickas inom kommunen och till externa parter, t.ex. via e-post, chattar, SMS och digitala möten. Riktlinjerna gäller för all sådan typ av kommunikation.

Digital kommunikation är vanligtvis inte krypterad och oskyddad. Till exempel kan ett e-postmeddelande utan kryptering jämföras med att skicka ett vykort. Det är dels därför viktigt att medvetet välja rätt teknisk lösning, så att den är lämpad för just den information som ska förmedlas och att kommunikationen sker på ett säkert sätt. Det är även viktigt att vara medveten om att det som sägs, visas eller skrivs kan kopieras eller spelas in, ibland även utan inblandade parter kännedom.

Örebro kommun har flera olika tekniska lösningar för att möta verksamheternas behov av att skicka och ta emot **konfidentiell** information. Om du behöver skicka konfidentiell information så är det viktigt att du tar reda på vilken lösning som är bäst lämpad.

Ansvar	
A.5.1	Den enskilde medarbetaren som är kontoinnehavare är ansvarig för den kommunikation som sker från kontot.
A.5.2	Medarbetaren är ansvarig för att löpande öppna, läsa och hantera inkommande meddelanden. Vid frånvaro, t.ex. semester, sjukfrånvaro eller föräldraledighet, ska autosvar användas, och om nödvändigt ska hänvisning göras till kollega eller chef. Vid avslut av anställning tas kontot bort.
A.5.3	E-postkonton som delas av flera, t.ex. myndighetsbrevlådor (för nämnder) och funktionsbrevlådor (t.ex. för enheter) ska ha utpekade ansvariga.
A.5.4	E-postkonton som delas av flera, t.ex. myndighetsbrevlådor (för nämnder) och funktionsbrevlådor (t.ex. för enheter) ska bevakas och inkommande e-post ska öppnas löpande, läsas och hanteras.
A.5.5	För arbetsrelaterad digital kommunikation ska alltid regler för registrering och hantering av allmänna handlingar följas.

Privat digital kommunikation	
A.5.7	Håll isär arbetsrelaterad och privat kommunikation. Använd inte ditt konto i Örebro kommun för privata ändamål, utan ha ett konto som du inte använder för ärenden kopplade till arbetet.
A.5.8	Det är inte tillåtet att automatiskt vidarebefordra e-post från kommunala e-postadresser till privata eller externa e-postadresser.

Konfidentiell information	
A.5.9	Konfidentiell information får endast kommuniceras med IT-resurs (t.ex. system, tjänst) som har, av Örebro kommun, godkänd kryptering.
A.5.10	Skanning av konfidentiell information ska ske på IT-resurs (t.ex. skrivare med skanningsfunktion) som har, av Örebro kommun, godkänd kryptering.
A.5.11	Konfidentiell information får aldrig anges i ämnesrad eller i kalenderbokningar. Detta gäller även vid användande av krypterad digital kommunikation.
A.5.12	Distansmöten som behandlar konfidentiell information får endast ske i, av Örebro kommun, godkänd IT-resurs.

A6. Lagring och säkerhetskopiering

Det är viktigt att information lagras på ett säkert sätt och säkerhetskopieras för att det ska vara möjligt att återskapa/återfå informationen i händelse av diskkrasch, oavsiktlig radering m.m.

Riktlinjer för lagring och säkerhetskopiering	
A.6.1	Endast av Örebro kommun godkända system och lagringsytor är tillåtna att användas. Kontrollera vilka system och lagringsytor som är tillåtna inom din verksamhet.
A.6.2	Konfidentiell 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.6.3	Lokal lagring av konfidentiell information, t.ex. på en persondator, får endast ske om lagringsenheten eller filerna är krypterade med, av Örebro kommun, godkänd metod för kryptering.
A.6.4	Information ska lagras på nätverket så att den säkerhetskopieras. Det kan vara i verksamhetssystem, gemensamma lagringsytor (t.ex. Teams) eller personliga lagringsytor (t.ex. OneDrive).
A.6.5	Om information behöver lagras på lokal hårddisk, se till att regelbundet kopiera över informationen till nätverket.
A.6.6	Om information har gått förlorad, exempelvis om man av misstag råkat radera ett dokument, ska Kommunsupport kontaktas. I vissa fall är det möjligt att återskapa informationen.
A.6.7	Fysiska dokument som innehåller konfidentiell information ska förvaras inlåsta i brand- och säkerhetsskåp.

Molntjänster är datortjänster som tillhandahålls över Internet, exempelvis lagring eller programvaror.

Riktlinjer för lagring i molntjänster	
A.6.8	Endast godkända molntjänster är tillåtna att användas. Kontrollera vilka molntjänster som är tillåtna inom din verksamhet.
A.6.9	Konfidentiell information får inte lagras i personliga molntjänster.

Lagring på mobila enheter, smarta telefoner och surfplattor

→ Se avsnitt A2. Mobila enheter

A7. Spårbarhet och loggning

Loggning sker i kommunens datorer och nätverk. Loggarna används för felsökning, utredning av incidenter, för att förhindra brott och kontrollera efterlevnad av regelverk. Loggarna lagras under en viss tid, och är åtkomliga endast för en begränsad grupp behöriga administratörer.

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. Örebro kommun har som arbetsgivare rätt att, 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.

A8. Säkert beteende

Kommunens information hanteras skriftligt, analogt på papper och digitalt, men även muntligt. Vi kommunicerar dagligen informellt och formellt och det är viktigt att vi betar oss med försiktighet och eftertanke när vi hanterar **konfidentiell** information. Tänk på att det alltid finns informell information som inte i förhand är definierad och klassad, utan som skapas i det ögonblick det uttalas eller skrivs.

Det är alltid viktigt att tänka på vilka som befinner sig i omgivningen och ifall de är behöriga att ta del av informationen som hanteras. Kretsen av behöriga är alltid begränsad för **konfidentiell** information. Det är därför viktigt att inga obehöriga kan se eller höra sådan information, i arbetet och i informella sammanhang.

Riktlinjer för muntlig information	
A.8.1	Konfidentiell information har en begränsad krets av behöriga. Detta måste beaktas så att inte obehöriga kan höra sådan information, både i arbetet och i informella sammanhang, t.ex. vid fikabordet. Samtal ska avskilt på ett sådant sätt att med- eller avlyssning försvåras, samt överhörning till intilliggande rum inte är möjlig.
A.8.2	Konfidentiell information bör inte kommuniceras muntligt i publika lokaler. Endast öppen information får kommuniceras hörbart utanför arbetsplatsen, exempelvis vid fysiska samtal på tåget eller i telefonsamtal i kassakön.

Riktlinjer för skriftlig information	
A.8.3	Skriftligt material som innehåller konfidentiell information får inte ligga framme så att obehöriga kan läsa och ta del av den. Materialet ska låsas in i godkända säkerhetsskåp när man lämnar arbetsplatsen, även för kortare stunder.
A.8.4	Konfidentiell information på skärm ska vara skyddad från obehöriga. Skärmen ska låsas när man lämnar datorn eller surfplattan, även för en kortare stund. Så kallat "smarkort" (i form t.ex. e-tjänstekort) ska tas ut från datorn när arbetsplatsen lämnas.
A.8.5	Besökare får inte vistas utan uppsikt i lokaler där konfidentiell information kan finnas. Mottagare av besök ansvarar för besökare så länge de befinner sig i kommunens lokaler. Obekanta personer i sådana lokaler ska tillfrågas vem de söker och vägledas rätt.
A.8.6	Vid fysisk post ska förslutna brev användas för intern information och rekommenderade försändelser ska användas om brev innehåller konfidentiell information.

A.8.7	Då konfidentiell 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.8.8	Vid utskrift ska dokument omgående hämtas upp ur skrivare. Vid utskrift av konfidentiell information ska utskriften övervakas så att man är säker på att ingen obehörig kan läsa informationen.
A.8.9	Pappersdokument som innehåller konfidentiell information måste vid kassering strimlas eller kastas i godkända säkerhetskärl.

B

Kapitel B: Styrning av informationssäkerhet

Innehåll Kapitel B

Kapitel B: Styrning av informationssäkerhet	22
Inledning	24
B1. Roller, ansvar och organisation.....	24
B2. Dokumentstruktur.....	26
B3. Informationsklassning	27
B4. Ledningssystem för informationssäkerhet	30
B5. Personalsäkerhet.....	31
B6. Leverantörsrelationer	32
B7. Efterlevnad och granskning	33

Inledning

Detta kapitel beskriver och reglerar hur arbetet med informationssäkerhet ska bedrivas i Örebro 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 de som arbetar med informations- och IT-säkerhet eller har ansvar för informationssäkerhet i förvaltningsobjekt, projekt, processer eller andra verksamheter.

Kapitlet kan även vara informativt för andra som är intresserade av hur arbetet med informationssäkerhet bedrivs i Örebro kommun, exempelvis sådana som arbetar med ledning och styrning av andra närliggande områden och processer. I kapitlet ges en introduktion till informationsklassning och den modell för informations-klassning som Örebro kommun antagit i och med dessa riktlinjer.

B1. Roller, ansvar och organisation

Grundprincip

Ansvaret för informationssäkerheten följer det ordinarie verksamhetsansvaret. Detta gäller från kommunledningen till den enskilde medarbetaren. Detta innebär att den som är ansvarig för en viss verksamhet (avdelning, enhet, process, projekt osv.) också är ansvarig för informationssäkerheten inom verksamhetsområdet.

Kommunens informationssäkerhetsstrateg och övriga som arbetar specifikt med informationssäkerhet, IT-säkerhet eller andra relaterade frågor fungerar som stöd för att medarbetare, verksamheter och kommunens ledning ska kunna ta ansvaret för informationssäkerheten.

Övergripande ansvar

Kommunfullmäktige beslutar om övergripande mål och inriktning för informationssäkerhet genom en kommunövergripande informationshanteringspolicy. Kommundirektören har ansvar för att informationssäkerhetsarbetet bedrivs i linje med den av kommunfullmäktige beslutade informationshanteringspolicyn. Kommundirektören beslutar om kommunövergripande riktlinjer för informationssäkerhet.

Grundprincipen är att ansvaret för informationshanteringen och informationssäkerheten följer det ordinarie verksamhetsansvaret. Verksamhetsansvarig ska därmed även skapa förutsättningar för att alla medarbetare ska kunna efterleva policyn och riktlinjerna. Verksamhetsansvariga bör fungera som förebilder och visa sitt stöd för dokumentens innehåll.

Ansvar inom respektive verksamhet

Varje nämnd är ytterst ansvarig för informationssäkerheten inom sitt verksamhetsområde. Nämnd kan vid behov besluta om instruktioner som kompletterar de centrala riktlinjerna för informationssäkerhet.

Verksamhetsansvarig, oavsett nivå, ansvarar för informationssäkerheten inom sin verksamhet. Varje verksamhetsansvarig att se till att sina medarbetare efterlever riktlinjer, har ett säkerhetsmedvetande och tillräcklig förståelse och kunskap för den informationssäkerhet som verksamheten behöver uppnå. Ansvar för informationssäkerhet kan i sig inte delegeras, däremot kan ansvaret att genomföra vissa arbetsuppgifter fördelas.

Medarbetares ansvar

Varje medarbetare har ansvar att följa Örebro kommuns riktlinjer för informationssäkerhet och eventuella verksamhetsspecifika regler. Medarbetaren har även skyldighet att rapportera informationssäkerhetsrelaterade brister och incidenter. Om någon bryter mot riktlinjerna för informationssäkerhet kan kommunens rutiner för disciplinärenden komma att tillämpas.

→ Riktlinjer för medarbetare återfinns i Kapitel A

Personuppgiftsansvar

Kommunstyrelsen och övriga nämnder är personuppgiftsansvariga, vilket innebär att de är ansvariga för de personuppgifter som behandlas inom deras respektive verksamhetsområden.

→ Se mer information om personuppgiftshantering och dataskydd i Riktlinjer för dataskydd.

Stadsarkivet

Arkivmyndigheten, det vill säga Kommunstyrelsen, har tillsynsansvar för att informationen hanteras enligt arkivlagen och kommunens interna styrdokument rörande informationens långsiktiga hantering och bevarande. Stadsarkivet är arkivmyndighetens verkställande enhet.

Objektägares ansvar

Objektägare ansvarar för att objekten efterlever informationshanteringspolicy och riktlinjer för informationssäkerhet. Informationssäkerhetsansvar hos specifika roller inom objektorganisationen beskrivs i Kapitel C.

I den mån det inte finns utpekade objektägare, t.ex. systemägare för ett system, 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 informationssäkerhetsfrågorna 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.

Informationsförsörjnings- och digitaliseringsavdelningens ansvar

Informationsförsörjnings- och digitaliseringsavdelningen ansvarar för att Örebro kommuns IT-miljö (så som tjänster, processer, system, infrastruktur och verktyg) har tillräcklig säkerhet, samt uppfyller krav från verksamheter, lagkrav och följer informationshanteringspolicy och riktlinjer för informationssäkerhet.

Informationssäkerhetsstrateg

Informationssäkerhetsarbetet i kommunen leds och samordnas av en informations-säkerhetsstrateg. Strategen ska utveckla ett systematiskt informationssäkerhetsarbete i Örebro kommun med hjälp av ledningssystem för informationssäkerhet (LIS) och kontrollera dess efterlevnad. Strategen leder Örebro kommuns informationssäkerhetsråd.

- ➔ **Se mer information om informationssäkerhetsstrategens roll och ansvar, samt informationssäkerhetsrådet i Rutin Styrning av LIS.**

Kommunens revisorer

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

B2. Dokumentstruktur

De dokument som är mest centrala för kommunens arbete med informationssäkerhet:

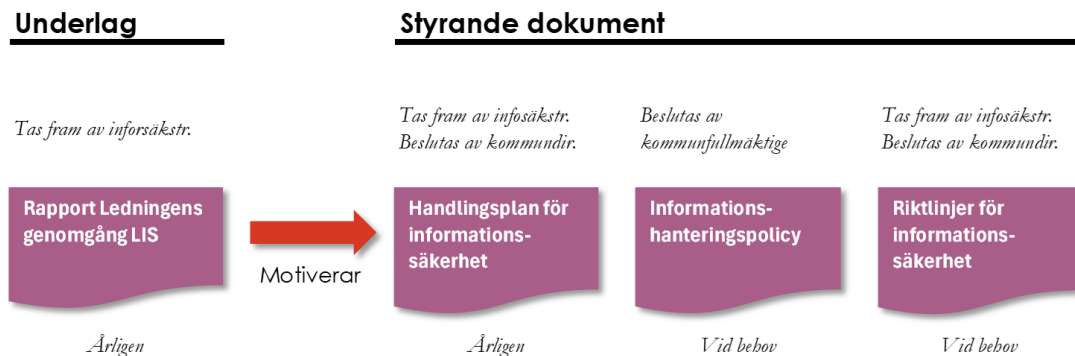
- Informationshanteringspolicy
- Riktlinjer för informationssäkerhet (detta dokument)
- Rapport Ledningens genomgång av LIS
- Handlingsplan för informationssäkerhet

Informationshanteringspolicy och *Riktlinjer för informationssäkerhet* (detta dokument) riktar sig till alla medarbetare inom Örebro kommun:

- **Informationshanteringspolicyn** är ett övergripande dokument som uttrycker ledningens viljeinriktning med informationshantering. I denna policy inkluderas informationssäkerhet och Örebro kommun har därför inget separat dokument för informationssäkerhetspolicy. Beslutas av Kommunfullmäktige och uppdateras vid behov.
- **Riktlinjer för informationssäkerhet** innehåller regler för hantering av information. Riktlinjerna är uppdelade i kapitel för olika målgrupper. Beslutas av kommundirektören och uppdateras vid behov.

Rapport Ledningens genomgång av LIS och *Handlingsplan för informationssäkerhet* riktar sig främst till de som arbetar med styrning av informationssäkerhet i Örebro kommun:

- **Rapport Ledningens genomgång av LIS** innehåller analys och genomlysning av informationssäkerheten i Örebro kommun. Rapporten tas fram årligen och ligger till grund till handlingsplaner, men även eventuella förändringar i policy och riktlinjer.
- **Handlingsplaner** för informationssäkerhet tas fram årligen och innehåller konkreta mål och åtgärder baserade på informationssäkerhetsanalysen.



Figur 3: Dokument för styrning av informationssäkerhet.

Modeller, metoder, vägledningar och andra stöddokument tas fram centralt för att stödja arbetet med informationssäkerhet på olika nivåer och för att underlätta tillämpning och efterlevnad av informationshanteringspolicy och riktlinjerna för informationssäkerhet.

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

Riktlinjer för dokumentstruktur för informationssäkerhet	
B.2.1	Örebro 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	Årliga handlingsplaner för informationssäkerhet ska tas fram baserade på informationssäkerhetsanalyser.
B.2.3	Det ska finnas en för organisationen övergripande informationssäkerhetspolicy som uttrycker ledningens viljeinriktning med informationssäkerhet. Örebro kommun har detta inkluderat i informationshanteringspolicy.
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 informationshanteringspolicy och riktlinjerna för informationssäkerhet.

B3. Informationsklassning

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

informationsmängder. 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, men även interna krav på informationens värde, känslighet och betydelse för Örebro kommuns verksamheter.

Att klassificera information på ett enhetligt sätt utifrån konfidentialitet, riktighet och tillgänglighet är en fundamental aktivitet i ett ledningssystem för informationssäkerhet (LIS) och ett krav i standarden SS-ISO/IEC 27001, vilken Örebro kommun avser att följa. Det är också en rekommendation från Myndigheten för samhällsskydd och beredskap (MSB) att organisationer ska klassa sin information och bygga sina säkerhetsåtgärder utifrån klasserna.

I den vägledande standarden SS-ISO/IEC 27002 rekommenderas framtagande av en organisationsgemensam *modell* för informationsklassning. En sådan modell 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.

Örebro kommuns modell för informationsklassning

Örebro kommun har i och med dessa riktlinjer antagit en egen modell för informationsklassning (Se Figur 4). Modellen baseras på Sveriges nationella modell för informationsklassning som är utgiven av MSB och SIS, men har anpassats till kommunens behov. Modellen innehåller kolumner för de tre aspekterna konfidentialitet, riktighet och tillgänglighet, samt rader för nivåer av skydds krav – normala (1) och **höga skydds krav** (2).

Kravnivå	Konfidentialitet	Riktighet	Tillgänglighet
2 Höga skydds krav	Konfidentiell information får endast vara tillgänglig för medarbetare som har särskild behörighet att hantera informationen.	Information som, om den ej är riktig och fullständig, kan medföra allvarliga konsekvenser för Örebro kommun, externa aktörer eller individer.	Information som, om den ej är tillgänglig, kan medföra allvarliga konsekvenser för Örebro kommun, externa aktörer eller individer.
1 Normala skydds krav	Intern information ska endast spridas till medarbetare inom Örebro kommun och till externa som har behov av informationen.	Information som, om den ej är riktig och fullständig, kan medföra måttlig negativ påverkan på Örebro kommun, externa aktörer eller individer.	Information som, om den ej är tillgänglig, kan medföra måttlig negativ påverkan på Örebro kommun, externa aktörer eller individer.
0 Inga skydds krav *	Öppen information kan spridas fritt inom och utom Örebro kommun.	*Alltid krav på att information ska vara riktig och tillgänglig!	

Figur 4: Örebro kommuns modell för informationsklassning

Idén med informationsklassning är att skydd ska anpassas till kraven på en viss informationsmängds 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. Information som klassas enligt modellen ska bedömas utifrån alla tre aspekterna, och 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	1	1	1
Patientjournal	2	2	2
Krisplan	1	2	2

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 skydds krav (2)	Kryptering	Tvåfaktors- autentisering	Speglning av databas
Normala skydds krav (1)	Inloggning med Användar-IT och lösenord	Inloggning med Användar-IT 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 skydds krav 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.

En viktig uppgift för objektägare och objektledare är sedan att systemklassa sina system så att skydds krav från informationsklassningen kan mötas och erhållas. Riktlinjer för detta finns i Kapitel C.

➔ Kapitel C – Riktlinjer för informationssäkerhet i verksamhetsnära förvaltning

Användningsområden och målgrupper

Modellen vänder sig dels till de i Örebro kommun som är verksamhetsansvariga och/eller ägare av information och objekt, dels till de som ansvarar för att rätt nivå av skydd skapas och upprätthålls. Den klassade informationen utgör ett underlag för en verksamhet vid kravställning av tjänster, exempelvis IT-tjänster, både internt och externt.

Klassningsmodellen kan därigenom fungera som ett gemensamt ramverk och kommunikationsmodell vid förhandling mellan beställare och leverantör av tjänster.

Identifiering och klassificering av information bör ske initialt när informationssäkerhetsbehovet ska analyseras, men även som ett led i löpande förbättring eller vid förändringar av verksamheter eller IT-system.

En mer utförlig vägledning, metodstöd och mallar för informationsklassning finns framtaget och publicerat på Örebro kommuns intranät.

Riktlinjer för informationsklassning	
B.3.1	Det ska finnas en för Örebro kommungemensam modell för informationsklassning.
B.3.2	Örebro 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.

B4. Ledningssystem för informationssäkerhet

Örebro kommun ska bedriva ett systematiskt informationssäkerhetsarbete med målet att skapa ett ledningssystem för informationssäkerhet (LIS). Ett LIS är ett etablerat begrepp för ett systematiskt arbete med informationssäkerhet och innebär en metodik som syftar till att upprätta, införa, driva, övervaka, granska, underhålla och förbättra organisationens informationssäkerhet. LIS avser här inte ett IT-baserat system, även om IT-stöd kan användas i delar av ett LIS.

Eftersom kommunen och dess omvärld är i ständig förändring är informationssäkerhetsbehovet dynamiskt och måste ständigt anpassas till exempelvis organisationsförändringar, nya lagar, nya hotbilder och strömningar i samhället. Det räcker därför inte att skapa en skydd som svarar mot interna och externa förutsättningar idag, eftersom dessa kan se annorlunda ut i morgon. Ett systematiskt arbete med informationssäkerhet genom 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 Örebro kommuns informationshanteringspolicy framgår att informationshanteringen ska byggas på standarder och andra tillförlitliga arbetssätt. Örebro kommuns informationssäkerhetsarbete ska baseras på standardserien SS-ISO/IEC 27000. Standardserien innefattar en stor mängd standarder, men två standarder kan sägas utgöra seriens huvudstandarder:

- **SS-ISO/IEC 27001:2023 – Informationsteknik – Säkerhetstekniker**
Ledningssystem för informationssäkerhet – krav. Denna standard ställer som namnet antyder krav på ett LIS, dvs. vad det ska innefatta. I standardens bilaga A finns ett antal säkerhetsåtgärder som tjänar som utgångspunkt för vilka säkerhetsåtgärder som ska finnas.
- **SS-ISO/IEC 27002:2022 – Informationsteknik – Säkerhetstekniker – Riktlinjer för informationssäkerhetsåtgärder.** Denna standard ger vägledning för införande av säkerhetsåtgärderna i föregående standards bilaga A.

Dessa båda standarder är i Sverige och internationellt dominerande ramverk för styrning av informationssäkerhet.

Standarderna i serien utgår från ett verksamhetsdrivet och riskorienterat arbete med informationssäkerhet, i motsats till ett teknikdrivet. Utgångspunkten är också att det är information som ska skyddas, utifrån de tre aspekterna konfidentialitet, riktighet och tillgänglighet, medan IT är resurser som används för att hantera informationen.

En etablerad och spridd standardserie innebär fördelar. Förutom att man tar tillvara samlade kunskaper och erfarenheter från hela världen så använder man ett gemensamt ramverk och en gemensam terminologi som underlättar vid kommunikation och samverkan med andra aktörer, exempelvis i samband med utbildning, revisioner och upphandlingar.

Riktlinjer för ledningssystem för informationssäkerhet (LIS)

B.4.1	Örebro kommun ska ha ett ledningssystem för informationssäkerhet.
-------	---

B5. Personalsäkerhet

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

Före och i samband med anställning

Bakgrundskontroll av sökande till tjänster i Örebro kommun ska ske genom verifiering av sökandes meritförteckning, t.ex. genom kontakt med referenser och bekräftelse av påstådda akademiska och yrkesmässiga kvalifikationer.

För vissa kritiska tjänster krävs en förstärkt kontroll i form av kreditupplysning och kontroll i brottsregister. Sådana kritiska tjänster är högre chefstjänster, säkerhetstjänster, eller för de som har åtkomst till känslig eller samhällsviktig information. Även lagsstiftningen om registerkontroll för skydd av barn och unga ska efterlevas.

För befattningar som har betydelse för rikets säkerhet, och således omfattas av Säkerhetsskyddslagen (1996:627), ska det i anställningsförfarandet genomföras en säkerhetsprövning. Prövningen ska genomföras innan en person genom anställning eller på annat sätt deltar i verksamhet som har betydelse för rikets säkerhet. Genomförande av säkerhetsprövning, när det är aktuellt att genomföras, samt för vilka befattningar framgår av Örebro kommuns säkerhetsskyddsplan. Prövningen administreras av Örebro kommuns säkerhetsavdelning.

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

Nyanställda ska delges ansvar och skyldigheter kopplade till informationssäkerhet, 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, t.ex. informationsägarskap. Tystnadsplikt för offentligt anställda regleras i offentlighets- och sekretesslagen. Alla som får tillgång till konfidentiell information ska informeras om detta och vilket ansvar som medföljer.

Riktlinjer för personalsäkerhet före och i samband med anställning	
B.5.1	Bakgrundskontroll av sökande ska göras före anställning där sökandes meritförteckning verifieras.
B.5.2	Anställning av kritiska roller ska genomgå förstärkt kontroll i form av kreditupplysning och kontroll i brottsregister.
B.5.3	För befattningar som har betydelse för rikets säkerhet, och som omfattas av Säkerhetsskyddslagen (1996:627) ska det i anställningsförfarandet genomföras en säkerhetsprövning.
B.5.4	Nyanställda ska 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. informationsägarskap.
B.5.5	Tillgång till konfidentiell information ska föregås av information om tystnadsplikt, sekretess och det ansvar som medföljer.

Under anställning

I enlighet med informationshanteringspolicyn ska medarbetare inom kommunen stärkas i sitt säkerhetsmedvetande och ha en förmåga att upprätthålla en god informationshantering i vardagen. Alla medarbetare och i förekommande fall externa aktörer ska erhålla lämplig utbildning för att kunna efterleva kommunens informationshanteringspolicy och riktlinjer för informations-säkerhet.

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.

I de fall anställda bryter mot gällande informationssäkerhetsriktlinjer ska dessa ärenden hanteras individuellt av ansvarig chef med stöd från personalavdelningen, på samma sätt som vid andra misskötselärenden.

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 informationshanteringspolicy 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	Det ska finnas en process för att vidta åtgärder mot anställda som har brutit mot gällande informationssäkerhetsriktlinjer.

Avslut eller ändring av anställning

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

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

Riktlinjer 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 tillträdande av roll.
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.

B6. Leverantörsrelationer

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

Riktlinjer för upphandling av IT-resurser återfinns i avsnitt D7. Riktlinjer för kontroll av IT-tjänst återfinns i avsnitt C9.

Riktlinjer för leverantörsrelationer	
B.6.1	Det ska finnas en vägledning med informationssäkerhetskrav som ska baseras på Örebro kommuns modell för informationsklassning. Vägledningen ska kunna användas som stöd vid extern upphandling av IT-tjänster.
B.6.2	Det ska finnas en vägledning 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.

B7. Efterlevnad och granskning

Efterlevnad av de styrande dokumenten för informationssäkerhet ska följas upp. I praktiken innebär det främst att metodstöd som är framtagna utifrån 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, objekt och IT-resurser med **höga skydds krav**.

Granskning och uppföljning av informationssäkerhet, och dess styrning, inkluderas i ledningssystemet för informationssäkerhet (LIS) och är en väsentlig del i ett LIS eftersom det direkt handlar om efterlevnadskontroll. Översyn och ev. revision av hela eller stora delar av Örebro kommuns informationssäkerhet ska göras minst vartannat år. Granskning av efterlevnad av informationssäkerhet bör också genomföras av extern part, exempelvis på uppdrag av Stadsrevisionen.

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

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).

Riktlinjer för efterlevnad och granskning av informationssäkerhet	
B.7.1	Efterlevnaden av styrdokument för informationssäkerhet ska följas upp.
B.7.2	Örebro kommuns informationssäkerhet ska utsättas för oberoende extern granskning.



Kapitel C: Informationssäkerhet i verksamhetsnära förvaltning

Innehåll Kapitel C

Kapitel C: Informationssäkerhet i verksamhetsnära förvaltning.....	34
Inledning	36
Roller och ansvar	36
C1. Dokumentation av informationssäkerhet	37
C2. Informationsklassning och systemklassning	37
C3. Behörigheter och logghantering	39
C4. Ändringshantering	40
C5. Användarinstruktioner	41
C6. Riskanalyser.....	41
C7. Incidenthantering	42
C8. Kontinuitetshantering	42
C9. Kontroll av IT-tjänst	43

Inledning

Örebro kommun har beslutat att tillämpa en modell för att förvalta och utveckling av digitala stöd, så kallad Styr- och samverkansmodell för hantering av digitala stöd. Det här kapitlet kompletterar med särskilda riktlinjer rörande informationssäkerhet i den verksamhetsnära förvaltningen och riktar sig främst till roller i denna. I Kapitel D som riktar sig till Örebro kommuns IT-verksamhet återfinns informationssäkerhetsrelaterade riktlinjer för den IT-nära förvaltningen.

Om man för ett system eller en systemgrupp ännu inte har börjat Styr- och samverkansmodellen så ska det ändå finnas en utsedd ägare för det aktuella systemet och som då ansvarar för säkerheten i systemet. De riktlinjer som finns i detta kapitel gäller även för dessa.

Roller och ansvar

Nedan beskrivs ansvar rörande informationssäkerhet för rollerna i den verksamhetsnära förvaltningen. Motsvarande ansvar för de IT-nära rollerna återfinns i Kapitel D – informations-säkerhet i IT-miljön. Som nämnts ovan är dessa ansvar tillägg till generella ansvar enligt Styr- och samverkansmodellen.

Objektägare

Objektägare är verksamhetens sammanhållande roll för att det digitala stödet som helhet fungerar för verksamheten. Objektägare säkerställer att Örebro kommuns gemensamma mål och strategier understöds av objektplan och att styrning sker i enlighet med dessa.

Objektägaren ansvarar för att Örebro kommuns informationshanteringspolicy och dessa riktlinjer efterlevs i objektet. Objektägaren ska besluta om objekts informationssäkerhetsnivåer genom att klassning sker i enlighet med Örebro kommuns modell för informationsklassning. Objektägaren ska tilldela tillräckligt med resurser i objektets förvaltningsplaner så att informationssäkerhetsnivån kan uppnås.

Objektledare

Objektledare verkställer objektplanen genom att styra, leda och följa upp objektuppdraget. I det ansvaret ingår att system eller grupper av system i förvaltningsobjekt klassas så att rätt skyddsnivåer uppnås, och att informationssäkerhetsrelaterade mål och åtgärder nås respektive genomförs. Objektledarens motsvarighet i den IT-nära förvaltningen är objektledare IT.

Objektledaren kan vid behov delegera arbetsuppgifter till objektproduktledare och objektsspecialist.

Objektproduktledare och objektspecialist

Objektproduktledaren och objektspecialist ska utföra informationssäkerhetsrelaterade aktiviteter på uppdrag av objektledare.

Informationsägare

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 objektägare ansvarar för, är normalt objektägaren även informationsägare. I de fall objektägaren inte också är informationsägare för informationen i objektet (t.ex. ett diariesystem som hanterar många olika slag av information), så är informationsägare i stället kravställare på objektägaren vad gäller säkerheten för den aktuella informationen.

C1. Dokumentation av informationssäkerhet

Informationssäkerhet ska vara en naturlig del i förvaltningen av objekt och de system som ingår i objekt. Säkerhetsförhållanden ska vara dokumenterade i systemsäkerhetsbeskrivningar och planerade säkerhetsåtgärder ska ingå i objektplan så att de formellt fastställs av objektägaren och har en budget.

Informationsrelaterade mål och åtgärder ska finnas med i objektsplaner. Mål och åtgärder kan uppkomma eller motiveras med exempelvis resultat från riskanalyser och revisioner, erfarenheter från inträffade incidenter eller krav i dessa riktlinjer.

Informationssäkerhet i förvaltningsplaner

C.1.1	Informationsrelaterade mål och åtgärder ska finnas med i objektplaner.
-------	--

Systemsäkerhetsbeskrivningar

Objekts säkerhetsförhållanden ska dokumenteras systemsäkerhetsbeskrivningar. En systemsäkerhetsbeskrivning ska finnas för varje system.

Av systemsäkerhetsbeskrivningen ska det framgå:

- Vilka informationsmängder 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)

Objektsäkerhetsbeskrivning

C.1.2	System ska ha en systemsäkerhetsbeskrivning där systemets informationssäkerhet är dokumenterad.
-------	---

C2. Informationsklassning och systemklassning

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 den får tillräckligt skydd, men ibland också för att undvika att information får onödigt överskydd med höga kostnader som följd. Även system ska klassas och då baserat på hur den

ingående informationen är klassad. Klassning av information och system ska ske i enlighet med Örebro kommuns modell för klassning som beskrivs i Kapitel B.

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

Vid en klassning ska informationen bedömas utifrån alla tre aspekterna; konfidentialitet, riktighet och tillgänglighet. Då får man fram en så kallad klassningsprofil. En informationsmängd kan till exempel vara mycket kritisk när det gäller riktighet och tillgänglighet, men mindre känslig när det gäller konfidentialitet. Den informationsmängden får då klassningsprofilen 1-2-2.

Klassning av ett system ska baseras på klassningen av den information som systemet hanterar. Ett system kan läggt ge den klassning som den ingående informationen har. Exempel:

Informationsmängder	Konfidentialitet	Riktighet	Tillgänglighet
Information 1	0	1	1
Information 2	1	2	1
Information 3	1	1	2
Systemklassning	1	2	2

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

Det viktiga är att kritisk information, dvs. information med höga skyddskrav i någon av de tre aspekterna, är identifierad och klassad så att tillräckligt skydd kan skapas för systemet.

Systemklassning utgör underlag vid kommunikation och kravställning mot den IT-nära förvaltningen eller mot externa leverantörer. Se särskilda säkerhetsåtgärder för system med **höga skyddskrav** i Kapitel D. Systemklassningen ger också ett underlag för hur användare kan och får arbeta i system. I Kapitel A finns hanteringsregler för medarbetare som påverkas av hur informationen är klassad.

Särskilda rutiner och regler ska upprättas för hantering av **konfidentiell** information, som exempelvis skyddade personuppgifter. Sådana rutiner och regler ska finnas med i användarinstruktioner (se avsnitt C5).

Riktlinjer för klassning av förvaltningsobjekt	
C.2.1	Kritiska informationsmängder i system ska vara inventerad och klassade enligt Örebro kommuns modell för informationsklassning.
C.2.2	System ska klassas som helhet baserat på den klassning som är gjord av information i systemet.
C.2.3	Särskilda rutiner och regler för ett system ska upprättas för hantering av konfidentiell information, som exempelvis skyddade personuppgifter.

C3. Behörigheter och logghantering

Behörighet, eller åtkomsträttigheter, definierar användares rätt att använda informationstillgångar och system för att t.ex. läsa, söka, skriva, radera, skapa eller köra ett program. För att få behörighet till information eller olika system måste användare först identifieras. Det görs genom att koppla användares identitet till ett unikt användar-ID. Inloggning innebär att användaren identifierar sig (autentiseras) med lösenord eller på andra sätt. Därefter kan användaren få tillgång till olika informationstillgångar eller system, beroende på vilka behörigheter som har kopplats till kontot.

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 i stället 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.

Objektägare ansvarar för beslut om hur behörighetstilldelning ska gå till, vilka som ska få tillgång till system som ingår i objekt och vilka behörigheter dessa ska ha. Verksamhetens och dess krav på informationens konfidentialitet och riktighet, tillsammans med rättsliga krav som lagar, föreskrifter och avtal, styr hur behörigheterna ska se ut.

För externa användare ska dessutom åtkomsttilldelningen vara tidsbegränsad för den tid som behövs för att utföra uppgiften, samt föregås av sekretessförbindelse.

Varje användare ska ha ett unikt Användar-ID. Gruppidentiteter är inte tillåtna (under vissa förutsättningar kan dock detta beviljas, se information under D.2.13).

Det ska finnas processer eller rutiner som underhåller och förvaltar behörighetstilldelning, exempelvis hantering av beställning, ändring och borttagning av behörigheter. Förändringar i användares roller måste återspeglas i processer och rutiner, t.ex. när användare byter arbetsuppgifter eller avslutar anställning.

För användare med särskilda åtkomsträttigheter (administratörer) ska revision ske med kortare intervall. Särskild uppmärksamhet kan behövas då medarbetare med särskilda åtkomsträttigheter slutar eller byter tjänst.

Sådana processer eller rutiner måste vara förankrade med den IT-nära förvaltningen så att tekniska förändringar genomförs. Objektägare IT ska säkerställa att de delar som rör införande, förändring och borttagning av åtkomst i IT-resurser följs. I Kapitel D finns riktlinjer för hur åtkomstkontroll ska ske i IT-miljön (avsnitt D2 – Styrning av åtkomst).

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 informationssäkerhetsändelser. Detta är särskilt viktigt, och obligatoriskt, om system hanterar information med **höga skydds krav** eller om regelstyrd behörighetshantering används.

När loggning används ska det finnas processer eller rutiner för dess hantering. Dessa ska innefatta hur loggning går till, hur loggar skyddas mot manipulation och obehörig åtkomst, hur länge de sparas och hur de granskas. Processer och rutiner för loggning ska följas upp och dokumenteras.

I de fall logginformation går att knyta till en enskild person är de att betrakta som personuppgifter och omfattas då av Dataskyddsförordningen.

Riktlinjer för behörigheter och logghantering	
C.3.1	Det ska finnas dokumenterade processer och/eller rutiner för hantering 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 i objekt.
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	Då regelstyrd behörighetshantering används i stället för teknisk behörighetshantering är loggning av användares aktiviteter obligatorisk.
C.3.7	Förändringar i anställningar och roller ska omedelbart rapporteras till personalavdelningen så att reglering sker i Personec.
C.3.8	Uppföljning ska ske av behörighetshantering och logghantering i objekt.

C4. Ändringshantering

Ändringshantering ska ske på ett strukturerat sätt för att säkra systemets säkerhet, funktionalitet och användbarhet och för att minimera antalet fel orsakade av förändringen. Till exempel kan ändringar bero på önskemål från verksamhet/användare, fel eller brister, förändringar i legala krav eller nya versioner från systemleverantörer.

Ändringar i system ska vara samordnade med Change management-processen inom den IT-nära förvaltningen. I Kapitel D finns riktlinjer som rör bl.a. systemtest och hantering av testdata (avsnitt D7 Anskaffning och utveckling av IT-resurser). Större förändringar i eller omkring ett system ska föregås av en riskanalys (se avsnitt C6 Riskanalys).

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

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).
-------	---

C5. Användarinstruktioner

Objektägare ansvarar för att det finns användarinstruktioner för samtliga användare till ett system. Användare ska utbildas enligt instruktionerna och instruktionernas efterlevnad ska kontrolleras. Användarinstruktionerna ska omfatta följande delar inom informationssäkerhet:

- Regler kring inloggning och lösenordshantering
- Behörigheter
- Särskilda instruktioner för hur **konfidentiell** information får hanteras.
- 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

Ytterligare riktlinjer för användare kan läsas i Kapitel A.

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.

C6. Riskanalyser

Risker är oönskade händelser som kan inträffa och som kan ha en negativ påverkan. En risk är en kombination av hur sannolikt det är att en händelse inträffar och vilken konsekvens som händelsen kan få.

Riskanalys ska genomföras vid större förändringar som sker i system eller i hur systemet hanteras. Händelser som motiverar att en riskanalys ska genomföras kan vara exempelvis; Större systemuppdateringar, nyutveckling, nya användargrupper eller extern åtkomst, ägarbyte av systemleverantör eller 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 objektplaner.

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 objektplaner.

C7. Incidenthantering

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

Incidenter kan delas in i två typer; mindre incidenter och allvarliga incidenter.

- 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 upprättas och lämpliga åtgärder ska vidtas.
- Allvarliga incidenter är större störningar i system som t.ex. ett längre avbrott, dataintrång eller påverkan av skadlig kod. En allvarlig incident kräver en utredning där dokumentation ska göras enligt rutin. Utredningen ska drivas av objektledare i samverkan med relevanta aktörer, inte minst Incident manager och Problem manager på Informationsförsörjnings- och digitaliseringsavdelningen.

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

Objektledare ska upprätta avbrottsplaner att använda vid större avbrott och som ska innehålla ansvarsförhållanden, kontaktpersoner, samt eskaleringsvägar till interna och externa aktörer. Här ska samverkan ske med den IT-nära förvaltningen.

Objektledare ska årligen sammanställa samtliga incidenter som är kopplade till system. Kvarstående åtgärdsbehov som inträffade incidenter medfört ska tas om hand i objektplaner.

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 objektet ska dokumenteras och sammanställas. Kvarstående åtgärdsbehov ska tas om hand i objektplaner.

C8. Kontinuitetshantering

Att system och tjänster är tillgängliga är avgörande för att en god kontinuitet ska kunna upprätthållas. Genom informationsklassning klargörs vilka behov verksamheten har på tillgänglighet av information och därmed vilka krav som ställs på kontinuitet. **Höga skydds krav** för tillgänglighet innebär högre krav på säkerhetskopiering och redundans.

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

Nyckelpersonsberoende ska undvikas och i den mån det framkommer att organisationen är beroende av nyckelpersoner ska detta åtgärdas t.ex. genom utbildning av ersättare.

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

C9. Kontroll av IT-tjänst

Korrekt informationssäkerhet ska säkerställas under hela livscykeln och innebär att objektägare 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 klassningar och analyser av information och system. 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 angående vägledning för kontroll av IT-tjänst.

Riktlinjer för kontroll av IT-tjänst	
C.9.1	Innan användande av en IT-tjänst ska det kontrolleras att tjänsten kan leverera rätt skydd för verksamhetens information.
C.9.2	Innan användande av en IT-tjänst ska Objektägare acceptera 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	Konfidentiell information får endast lagras i en IT-tjänst som är kontrollerad, risken acceptabel och att lagringen av information inte bryter mot lag.
C.9.5	IT-tjänster som lagrar konfidentiell information ska kontrolleras minst en gång per år.

D

Kapitel D: Informationssäkerhet i IT-miljön

Innehåll Kapitel D

Kapitel D: Informationssäkerhet i IT-miljön	44
Inledning	46
Roller och Ansvar	46
D1. Hantering av tillgångar	47
D2. Styrning av åtkomst	49
D3. Kryptering.....	52
D4. Fysisk och miljörelaterad säkerhet	53
D5. Driftsäkerhet.....	56
D6. Kommunikationssäkerhet	60
D7. Anskaffning och utveckling av IT-resurser	62
D8. Informationssäkerhetsincidenter	65
D9. IT-relaterad kontinuitetshantering	67
D10. Granskning och kontroll.....	68

Inledning

Detta kapitel innehåller riktlinjer rörande säkerhet Örebro kommuns IT-miljö. Riktlinjerna vänder sig därför främst till chefer och medarbetare inom Örebro kommuns informationsförsörjnings- och digitaliseringsavdelning. Riktlinjerna riktar sig också till externa parter som arbetar på uppdrag åt Örebro kommun, exempelvis inhyrda konsulter.

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

Kraven baseras på standarden SS-ISO/IEC 27002:2014 som till största delar innehåller säkerhet i IT-miljöer:

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 Örebro kommuns klassningsmodell (se Kapitel B). IT-resurser som hanterar information ska ges ett skydd i enlighet med dessa skydds krav. Särskilda regler gäller i vissa fall för information som klassats enligt **höga skydds krav** i en eller flera av aspekterna konfidentialitet, riktighet och tillgänglighet. Detta markeras genomgående med fetstil och rader i tabeller med riktlinjer har dubblade linjer.

Roller och Ansvar

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

Ytterst ligger ansvaret på Informationsförsörjnings- och digitaliseringsdirektören i egenskap av chef för informationsförsörjnings- och digitaliseringsavdelningen och som ägare av styrprocessen *Styra och leda för en säker informationshantering i kommunen* och underliggande delprocesser. Därigenom är Informationsförsörjnings- och digitaliseringsdirektören ytterst ansvarig för att säkerheten i informationshantering och IT-miljö som tjänster, processer, system, infrastruktur, verktyg etc. är tillräcklig och uppfyller verksamhetens krav, legala krav samt informationssäkerhetspolicyn och dessa riktlinjer för informationssäkerhet.

Örebro kommun har beslutat att tillämpa en modell för att förvalta och utveckling av digitala stöd, så kallad Styr- och samverkansmodell för hantering av digitala stöd. Detta kapitel kompletterar med särskilda riktlinjer rörande informationssäkerhet i den IT-nära förvaltningen. Kapitel C riktar sig till den verksamhetsnära förvaltningen och innehåller informationssäkerhetsrelaterade riktlinjer för denna.

IT-säkerhetssamordnare

IT-säkerhetssamordnaren samordnar arbetet med säkerheten i Örebro kommuns IT-miljö och är stödjande vid kravställning på externa aktörer. Ansvar för säkerheten i IT-resurser ligger inte på IT-säkerhetssamordnare, utan dennes roll är att kravställa, stödja och kontrollera arbetet med att nå och upprätthålla rätt nivåer av säkerhet i dessa.

→ Se mer information om IT-säkerhetssamordnarens roll och ansvar i **Rutin Styrning av LIS**.

Objektägare IT

Objektägare IT ansvarar för att IT-säkerheten i system överensstämmer med verksamhetens krav så att rätt säkerhetsnivå upprätthålls och att aktuella IT-resurser ges ett skydd som motiveras av klassningen av system. Objektägare IT:s motsvarighet i den verksamhetsnära förvaltningen är objektägare verksamhet.

Objektägare IT ansvarar för att Örebro kommuns informationshanteringspolicy och dessa riktlinjer efterlevs i objekten.

Objektledare IT

Objektledare IT samverkar med objektledare verksamhet och i det ansvaret ingår att IT-säkerhetsrelaterade mål och åtgärder i objektverksamheten nås respektive genomförs.

Objektägare av IKT-objekt

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

IT-specialister

IT-specialister ansvarar för att utföra IT-säkerhetsrelaterade aktiviteter på uppdrag av objektägare IT, objektledare IT, ägare av IKT-objekt eller IT-säkerhetssamordnare, eller andra chefer och ansvariga inom informationsförsörjnings- och digitaliseringsavdelningen.

D1. Hantering av tillgångar

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, exempelvis i ett CMDB (Configuration Management Database).

Förvaltningsobjekt som omfattas av förvaltningsorganisationen, exempelvis verksamhetssystem, har naturliga ägare inom Informationsförsörjnings- och digitaliseringsavdelningen i form av objektägare IT. Andra IT-resurser, som underliggande infrastruktur, stödsystem m.m., ingår i IKT-objekt och ska ha utpekade ägare.

Klassning av IT-resurser

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

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

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

Användningsinstruktioner

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

Regler och instruktioner kan exempelvis avse användning av:

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

Riktlinjer för hantering av tillgångar	
D.1.1	Samtliga IT-resurser ska identifieras och tilldelas en ägare med rollerna Objektägare IT eller IKT-objektägare.
D.1.2	En komplett förteckning över samtliga IT-resurser ska upprättas och underhållas, exempelvis i ett s.k. CMDB. Rutiner ska finnas för att hålla förteckningen aktuell och den ska skyddas från åtkomst eller förändring av obehörig.
D.1.3	IT-resurser ska klassas baserat på klassningen av den information som hanteras i IT resursen och/eller baserat på klassningen av andra objekt som IT-resursen stödjer eller påverkar.
D.1.4	Skyddsåtgärder i en IT-resurs ska motsvara dess klassning så att rätt nivå av IT-säkerhet upprätthålls under IT-resursens hela livscykel, såväl vid införande, under drift som efter avveckling.

D.1.5	Informationssäkerhetskrav som gäller användandet av IT-resurser ska förmedlas till användare i form av användningsinstruktioner.
-------	--

D2. Styrning av åtkomst

Styrning av åtkomst är grundläggande för att skydda information och IT-resurser. Behörigheter innebär vissa rättigheter att använda en informationstillgång (t.ex. 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 använda ett program.

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

Det kan vara svårt att på förhand definiera arbetsuppgifter och behov. Det kan även i akuta situationer vara nödvändigt att annan personal än den ordinarie snabbt behöver ha åtkomst till informationen. I dessa fall kan teknisk behörighet behövas till en stor mängd information eller IT-resurser. Då får teknisk åtkomstkontroll ersättas av regelstyrd åtkomstkontroll, där regler säger att man inte får ta del av information som inte rör ens aktuella arbetsuppgifter. I sådana system är det särskilt viktigt med funktioner för uppföljning, övervakning och loggning.

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

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

Identifiering och autentisering

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

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

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

Stark autentisering är också krav vid extern åtkomst till Örebro 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.

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 folkbokföringen.
D.2.3	Vid åtkomst till information med höga skydds krav avseende konfidentialitet eller riktighet ska stark autentisering användas.
D.2.4	Stark autentisering är krav vid fjärråtkomst till Örebro kommuns IT-miljö.
D.2.5	Fjärråtkomst för inloggning med administrativa (priviligierade) konton till IT-resurs med höga skydds krav avseende konfidentialitet eller riktighet är inte tillåten.
D.2.6	Lösenord är alltid konfidentiell information som har höga skydds krav 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: <ul style="list-style-type: none"> • Tekniska funktioner implementeras där så är möjligt i IT-resursen för att säkerställa att lösenordsregler för medarbetare avseende historik, komplexitet och åldring av lösenord följs. • Lösenord ska aldrig skickas/transporteras i klartext över nätverk. I de fall detta inte är möjligt ska tillfälliga lösenord i kombination med tvingande lösenordsbyte användas. Tillfälliga lösenord ska enbart vara giltiga för en (1) inloggning. • Lösenord får aldrig lagras på ett sätt som gör det möjligt att dekryptera dem till klartext, om möjligt ska hash-funktion med salt användas. Om felaktigt lösenord används mer än fem gånger ska aktuellt användar-ID utestängas en viss tid ur systemet och händelsen loggas.
D.2.7	För att minska risken för obehörig åtkomst ska samtliga klienter (datorer samt mobila enheter) förses med låsskärm så att skärm automatiskt låses efter en definierad tids inaktivitet och enbart kan aktiveras igen genom en förnyad autentisering.

Reglering av åtkomsträttigheter

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 objektägare eller objektledare i verksamheten som beslutar vilka som ska få tillgång till systemet och vilka behörigheter dessa ska ha, samt hur systemet är klassat. Objektägare IT ansvarar för att upprätta ett BKS som motsvarar dessa krav.

Det ska finnas beslutade och dokumenterade regler och rutiner för behörighetshandling, dvs. BKS, för IT-resurser. Detta inkluderar att underhålla och förvalta behörigheter, exempelvis handtering av beställning, ändring och borttagning av behörigheter och rättigheter. Förändringar i användares roller måste återspeglas i behörighetshandlingen, t.ex. när användare får andra arbetsuppgifter eller avslutar sin anställning.

Det ska finnas rutiner som säkerställer att reglering av åtkomst sker vid anställning, vid förändring av roll eller arbetsuppgifter samt vid upphörande av anställning.

Innan användare som är anställd inom Örebro kommun tilldelas åtkomst till IT-resurs som innehåller konfidentiella uppgifter och information, ska den enskilde informeras om detta och vilket ansvar som medföljer.

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

För administrativa åtkomsträttigheter gäller att de ska vara restriktiva och ges endast till dem som behöver de för att utföra sitt uppdrag. I de fall som funktion för privilegiehöjning finns ska sådan användas, t.ex. genom att använda ”sudo” i Linux/Unix eller använda separat konto med förhöjda rättigheter i Windows. Vidare ska säkerställas att automatisk utloggning sker efter en definierad tid. Tiden bör vara kortare än för normala användare.

Regelbunden uppföljning och revision av samtliga åtkomsträttigheter ska ske kontinuerligt. För privilegierade användare med särskilda åtkomsträttigheter (administratörer) ska revision ske med tätare regelbundenhet än andra användare. Särskild uppmärksamhet kan behöva ägnas när medarbetare med privilegierade åtkomsträttigheter slutar eller byter tjänst. Processer och rutiner för behörighetshantering ska följas upp och dokumenteras.

Riktlinjer för reglering av åtkomsträttigheter	
D.2.8	Det ska finnas beslutade och dokumenterade regler och rutiner för behörighetshantering till IT-resurser med BKS.
D.2.9	IT-resurser ska ha åtkomsträttigheter som motsvarar IT-resursernas klassningsnivå.
D.2.10	Användaridentiteter och vilka individer dessa tillhör ska registreras i en gemensam förteckning och rutin ska finnas för att hålla denna förteckning uppdaterad. För att garantera spårbarhet ska rutinen även innehålla kontroll så att inte tidigare identiteter återanvänds. Historikfunktion ska finnas så att förteckningen kan visa vilka identiteter som fanns och vilka individer dessa tillhörde vid varje given tidpunkt.
D.2.11	Åtkomst av IT-resurser ska vara registrerade i en förteckning med den åtkomst som beslutats och rutin ska finnas att hålla denna förteckning uppdaterad. Historikfunktion ska finnas så att förteckningen kan visa vilka identiteter och individer som hade åtkomst till en IT-resurs vid en given tidpunkt.
D.2.12	Åtkomst som inte längre behövs eller behov av ny åtkomst ska regleras skyndsamt. För betydande IT-resurser ska åtkomst justeras inom en arbetsdag.
D.2.13	Det ska finnas rutiner för att säkerställa att reglering av åtkomst sker vid förändrad roll, förändrade arbetsuppgifter eller vid upphörande av anställning.
D.2.14	Administrativa rättigheter ska tilldelas restriktivt, vara motiverade och tidsbegränsade. För tilldelning av administrativa rättigheter för användare på klienter gäller att den ska antingen vara tillfällig för en specifik uppgift och upphöra när uppgiften är slutförd, eller vara tidsbegränsad med angivet slutdatum. Objektägare verksamhet och Objektägare IT beslutar om tilldelning av privilegierad åtkomsträtt. Granskning av administrativa rättigheter ska ske regelbundet.
D.2.15	Gruppidentiteter är generellt inte tillåtna. Eventuella undantag ska godkännas av både Objektägare verksamhet och Objektägare IT. Gruppidentiteter ska enbart beviljas under följande förutsättningar: <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.2.16	Externa identiteter ska kunna särskiljas från interna identiteter. För externa användare gäller utöver övriga regler för åtkomsttilldelning även att tilldelning av åtkomst ska: <ul style="list-style-type: none"> • Tidsbegränsas att endast omfatta tiden som behövs för att utföra uppgiften. • Föregås av sekretessförbindelse.
D.2.17	Användare som tilldelas åtkomst till IT-resurs som innehåller information med höga skydds krav avseende konfidentialitet, ska informeras om detta och vilket ansvar som medföljer.
D.2.18	Prövning av den enskilde ska ske, om befattningen kräver det, och en tystnads- och sekretessförbindelse upprättas innan åtkomst tilldelas till IT-resurs som innehåller information med höga skydds krav avseende konfidentialitet.

Säkerhetsloggning

För att erhålla spårbarhet och möjliggöra incidentutredningar och att i efterhand kunna utreda vad som hänt och för att upptäcka avvikelser från kommunens regelverk ska kommunens IT-resurser övervakas och loggas avseende användaraktiviteter, avvikelser, fel och informations-säkerhets händelser. 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, direkt eller indirekt, är det att anse som en personuppgift och omfattas därför av dataskyddsförordningen. För att en behandling av personuppgifter ska vara tillåten krävs att det finns laglig grund för den i artikel 6 dataskyddsförordningen. I de fall behandlingen innebär höga risker för de registrerades fri- och rättigheter ska en konsekvensbedömning avseende dataskydd genomföras. Notera att om loggning används för att tekniskt övervaka ett system av säkerhetsskäl får loggen inte användas för andra syften än dessa, utan att en ny laglighetsprövning samt eventuell konsekvensbedömning genomförs.

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

D3. Kryptering

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

Informationsförsörjnings- och digitaliseringsavdelningen ska vid behov tillhandahålla godkända krypteringslösningar med instruktioner. Behov av kryptering ska baseras på informationsklassning. Normalt finns behov av kryptering då det föreligger **höga skydds krav** på konfidentialitet och/eller riktighet.

Krypteringslösningar ska bygga på etablerade standarder som NIST 140–3 eller ISO/IEC 18033 och ska tas fram i samråd mellan Objektägare verksamhet, Objektägare IT och IT-säkerhetssamordnare. Införande av krypteringslösningar ska godkännas av Informationsförsörjnings- och digitaliseringsdirektör.

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

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

Riktlinjer för kryptering	
D.3.1	Krypteringslösningar ska baseras på etablerade standarder och införande ska godkännas av Informationsförsörjnings- och digitaliseringsdirektör.
D.3.2	Nyckelhantering ska säkerställas för att tillgodose de krav som finns för IT-resurs avseende <ul style="list-style-type: none"> • Revokering av nycklar • Validering av nycklars giltighet och autenticitet • Återställning av nycklar
D.3.3	Krypteringsnycklar är konfidentiell information och ska skyddas.

D4. Fysisk och miljörelaterad säkerhet

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, kontorsutrymmen där känslig information bearbetas samt arkiv. För IT-funktioner är det främst datorhallar, serverrum samt korskopplingsutrymmen som är aktuella.

Tillträden till säkra utrymmen ska vara restriktiva och endast ges till de personer som behöver tillträde för att utföra sitt uppdrag i den roll de har. Det ska finnas dokumenterade beslut om vem som ges tillträde att arbeta i säkra utrymmen.

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 etc. VA-dragningar i eller i direkt närhet av driftmiljö ska undvikas och risker för vatteninträngning hanteras. Om golvbrunn finns ska åtgärder vidtas för att undvika att vatten kan tränga upp.

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

Säkra utrymmen som innehåller IT-resurser med **höga skyddskrav** ska bevakas och fysisk närvaro ska loggas (t.ex. 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 egen personal vid leveranstillfället och eventuella avvikelser från förväntad leverans ska kvitteras av leverantören.

Underhåll, reparation och avveckling

Underhåll av utrustning ska ske i enlighet med leverantörens anvisningar.

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

Om underhåll och reparation ska utföras av utomstående på IT-resurs med **höga skyddskrav** avseende konfidentialitet ska vederbörande alltid underteckna sekretessförbindelse. Det kan ibland vara nödvändigt att vidta särskilda åtgärder, t.ex. att känslig information flyttas, raderas eller krypteras innan någon utomstående hanterar utrustningen. Detsamma gäller avveckling av 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 t.ex. behöva skrivas över eller destrueras på ett säkert sätt innan den sänds till skrotning eller återanvändning.

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, t.ex. där många externa personer frekvent vistas och i publika lokaler. Där krävs stöldskydd (t.ex. fastlåsning) och märkning.

Speciellt utsatt är också mobil utrustning där risken för förlust, stöld och skada är högre. Därför ska mobil utrustning som är avsedd att användas utanför kommunens lokaler förses med stöldskydd och märkning. Användning ska ske i enlighet med de instruktioner som gäller

vid distansarbete och mobil utrustning där användare t.ex. ska säkerställa att utrustning antingen övervakas eller låses in för att minska risken för stöld.

Elförsörjning

Säker elförsörjning (t.ex. 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.

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 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 registreras 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 vatteninträning 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	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	Datamedia som innehåller för verksamheten kritisk information och systeminformation ska förvaras i för datamedia brandklassat datamedieskåp.
D.4.14	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 sekretessförbindelse tecknas. Vid känslig information döljas, flyttas eller raderas från utrustningen. Underhåll och reparation ska följas upp i loggböcker.
D.4.15	Avveckling eller skrotning av IT-resurser och datamedia ska, efter att information som ska bevaras ha förts över till Stadsarkivet, ske genom att information skrivs över, raderas eller förstörs.
D.4.16	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.

D.4.17	IT-utrustning ska inte avlägsnas utanför kommunens lokaler utan tillstånd.
D.4.18	IT-utrustning tillhörande kommunen avsedd att användas utanför kommunens lokaler ska förses med stöldskydd och märkning

D5. Driftsäkerhet

Driftsrutiner

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

- installation och konfiguration av system,
- uppstarts- och nedtagningsrutin,
- säkerhetskopiering (se nedan),
- underhåll av utrustning,
- supportkontakter vid oväntade funktionella eller tekniska problem,
- hantering av media och
- datahall (se avsnitt D4 – Fysisk och miljörelaterad säkerhet).

Driftsrutiner ska vara formella, beslutade och dokumenterade.

Förändringar i IT-resurser ska styras enligt fastställd Change Management-process. 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 driftsmiljöer ska vara separerade för att minska risken för obehörig åtkomst eller ändringar i driftsmiljön.

Riktlinjer för driftsrutiner	
D.5.1	Det ska finnas formella, beslutade och dokumenterade driftsrutiner för väsentliga processer och objekt. Dessa ska göras tillgängliga för alla användare som behöver dem.
D.5.2	Ändringar i IT-resurser ska följa fastställd process som säkerställer att ändringarna är riskbedömda, planerade, kommunicerade, testade och godkända (ITIL Change Management).
D.5.3	Utvecklings-, test- och driftsmiljöer ska vara separerade för att minska risken för obehörig åtkomst eller ändringar i driftsmiljön.

Skydd mot skadlig kod

För att skydda mot skadlig kod behövs metoder för att förebygga och upptäcka skadlig kod, samt 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 A3 – Skadlig kod).

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

Programvara ska i förebyggande syfte skanna efter skadlig kod i

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

IT-resurser med **höga skydds krav** ska regelbundet granskas avseende skadlig kod.

Det ska finnas en fastställd rutin för återställning av IT-resurser (se avsnitt D9 – IT-relaterad kontinuitetshantering) som kan användas ifall angrepp av skadlig kod inträffar.

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).

Riktlinjer för skadlig kod	
D.5.4	Det ska finnas metoder och programvara för att förebygga och upptäcka skadlig kod, samt för att återställa kommunens IT-miljö efter angrepp. Alla datorer (servrar och klienter) ska ha skydd mot skadlig kod (antivirusprogramvara) som dagligen uppdateras, frekvent och regelbundet uppdateras.
D.5.5	IT-resurser som stödjer objekt med höga skydds krav ska regelbundet granskas avseende 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.
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).

Säkerhetskopiering

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 av information.

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

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

Vilka skyddsåtgärder som vidtas för specifika system ska styras på av hur de är klassade i aspekterna tillgänglighet och riktighet. Stöd för detta kan vara att använda de två måtten RPO

och RTO. Hur stor informationsförlust som kan accepteras kan definieras för varje IT-resurs genom att fastställa RPO (Recovery Point Objective). Den längsta acceptabla tiden för att återställa IT-resursen efter ett avbrott kan fastställas med målsättning för återställningstid RTO (Recovery Time Objective).

Säkerhetskopior ska lagras geografiskt åtskilt från originalmaterialet för att skydda från fysiska incidenter och katastrofer som t.ex. brand och översvämning. Ofta används lösningar där enbart långtidslagringen är skild från originalmaterialet. I de fallen bör korttidslagring skyddas genom ett säkert utrymme avsett för datamedia. Detta för att minimera risken att vid t.ex. brand förlora all information som tillförts systemet sedan kopiering till långtidslagring skedde (se avsnitt D4 – Fysisk och miljörelaterad säkerhet).

I de fall information hanteras i en molntjänst bör säkerhetskopior göras på informationen, applikationer och system i molntjänstmiljö. Vid användning av tjänstens egen funktion för säkerhetskopiering ska Örebro kommun säkerställa att krav på säkerhetskopiering har uppfyllts.

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

Riktlinjer för säkerhetskopiering	
D.5.9	För IT-resurser med höga skyddskrav avseende tillgänglighet ska redundans finnas i delkomponenter, system, lagring och nätverk samt säkerställd infrastruktur för IT-drift, t.ex. UPS elförsörjning, reservkraft, redundant kyla m.m. Tillgänglighet ska övervakas med automatiska larm som larmar om viktiga kvalitetsmått inte uppfylls. Gränsvärden för larm ska sättas så att mål för återställningstid säkerställs. Automatiska larm ska regelbundet testas.
D.5.10	Krav ska definieras för säkerhetskopiering av information baserat på klassning av riktighet och tillgänglighet. Dessa krav ska minst reglera vilken information som ska omfattas av säkerhetskopiering, hur lång tid som säkerhetskopior ska sparas, samt vilka kontroller som ska genomföras av att säkerhetskopiorna fungerar. Maximal informationsförlust och målsättning för återställningstid ska definieras för varje IT-resurs och tillsammans med övriga krav ligga till grund för vald lösning för säkerhetskopiering. <ul style="list-style-type: none"> • Målsättning för återställning av data, d.v.s. den maximalt acceptabla mängden av dataförlust som tillåts vid en återställning av en IT-tjänst efter ett avbrott (RPO), ska fastställas • Målsättning för återställningstid, d.v.s. den längsta acceptabla tiden för att återställa IT resursen efter ett avbrott (RTO), ska fastställas
D.5.11	Det ska finnas en process för återställning från säkerhetskopia som är testad och dokumenterad för respektive IT-resurs.
D.5.12	Säkerhetskopiering av IT resurser med höga skyddskrav avseende tillgänglighet (höga RTO krav) ska lagras på lämplig media för att skyndsamt kunna återställas. Övervakning av funktionen ska konfigureras med automatlarm.
D.5.13	Säkerhetskopiering av information med höga skyddskrav avseende konfidentialitet ska ske krypterat 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.5.14	Säkerhetskopior ska lagras geografiskt åtskilt från originalmaterialet. Om lösning används där man skiljer på långtids- och korttidslagring är det tillräckligt att långtidslagringen är skild från originalmaterialet under förutsättning att korttidslagrade säkerhetskopior förvaras i ett säkert utrymme avsett för datamedia.

Loggning och övervakning

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

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

Händelseloggar kan innehålla bl.a.

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

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

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

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

Riktlinjer för loggning och övervakning	
D.5.15	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 objektägares krav.
D.5.16	För att säkerställa all typ av loggning av händelser ska systemklockorna i alla relevanta IT-resurser synkroniseras mot en betrodd referenskälla för korrekt tid.
D.5.17	Loggningsverktyg och logginformation har höga skydds krav och ska skyddas mot manipulation och obehörig åtkomst.

Hantering av tekniska sårbarheter

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

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

Riktlinjer för hantering av tekniska sårbarheter	
D.5.20	Det ska finnas rutiner för att få information om, upptäcka, analysera och åtgärda tekniska sårbarheter i IT-resurser. Uppdateringar och säkerhetsuppdateringar ska göras regelbundet på IT-resurser.
D.5.21	I de fall säkerhetsuppdateringar inte är praktiskt möjlig, t.ex. för inbyggda eller SCADA-system, ska information om tekniska sårbarheter i sådana IT-resurser inhämtas och analyseras och lämpliga åtgärder vidtas för att hantera den tillhörande risken.
D.5.22	Säkerhetsgranskning av IT-resurser som exponeras mot Internet ska ske regelbundet och minst en gång per år för att kontrollera att inga uppenbara sårbarheter exponeras och att tillräcklig säkerhetsnivå upprätthålls. Sådan granskning kan t.ex. bestå av skanning av sårbarheter med automatiserade verktyg eller så kallade penetrationstester.
D.5.23	Det ska finnas regler för programinstallationer som definierar på vilket sätt som installationer ska utföras.

D6. Kommunikationssäkerhet

Kommunikationssäkerhet är skydd i IT-resurser och nätverk som används för data-kommunikation. Syftet är att skydda den information som kommuniceras.

Nätverkssäkerhet

Nätverk ska hanteras och styras för att skydda information i anslutna system och tillämpningar. Det ska finnas rutiner för hur nätverk hanteras och förvaltas av ansvarig objektorganisation.

Skyddsåtgärder ska införas för att nå säkerhet för information i nätverk och anslutna tjänster, baserat på klassningen av anslutna objekt, dvs. krav på konfidentialitet, riktighet och tillgänglighet. Krav på skydd ska inkluderas i avtal för nätverkstjänster om dessa tjänster tillhandahålls som outsourcade tjänster. Skydd för nätverkssäkerhet kan exempelvis vara:

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

Segmentering av nätverk ska användas som en del av den totala säkerhetslösningen för att skydda känslig information och övriga resurser. En grundläggande segmentering av nätverket innebär att skilja interna nät från Internet, interna nät mellan olika verksamheter i organisationen, samt skilja 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.

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	Segmentering av nätverket ska göras för att skilja interna nät från Internet, interna nät mellan olika verksamheter i organisationen, samt 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. • Dokumenterade kommunikationskontrakt ska upprättas mellan ägare för samtliga IT-resurser med kommunikation mellan olika segment. Kontrakten ska innehålla detaljerad information om vilka IT-resurser som ska kommunicera och vilka nätverksprotokoll och portar som ska användas. En rutin ska finnas för att uppdatera dessa kontrakt vid förändringar.
D.6.4	Brandväggar ska konfigureras i enlighet med dokumenterad brandväggspolicy. Av brandväggspolicyn ska framgå vilka nätverkstjänster som ska tillåtas, vilka händelser och aktiviteter som ska loggas och följas upp. Brandväggar och brandväggspolicier ska revideras regelbundet.
D.6.5	Kommunikationstjänster mellan Örebro kommun och externa nätverk ska dokumenteras och godkännas av Objektägare IT innan inkoppling får ske.

Informationsöverföring

Information som hanteras genom elektronisk meddelandehantering ska ges lämpligt skydd. I de fall som information med **höga skydds krav** avseende konfidentialitet ska skickas så ska lösning med kryptering och autentisering används.

Avtal som reglerar säker överföring av verksamhetsinformation mellan Örebro kommun och extern part ska upprättas.

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 med lämplig nivå av autentisering.
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 Örebro kommun och externa parter ska regleras genom avtal där minst följande regleras: <ul style="list-style-type: none"> • Motparten informeras om informationens klassning och garanterar att information med normala eller höga skydds krav avseende konfidentialitet ges rätt nivå av skydd och inte förs vidare till annan part.

	<ul style="list-style-type: none"> • Kommunikationslösning ska definieras med de nätverkskomponenter som ingår i säkerhetslösningen samt den konfiguration och de inställningar som krävs för att upprätthålla rätt nivå av skydd. • Vid kommunikation med annan part med normala eller höga skydds krav avseende konfidentialitet ska överföringen skyddas med kryptering. • Trafik i uppsatta förbindelser ska loggas av båda parter.
D.6.9	Kommunikation till extern part skyddas genom att konfigurera och aktivera standardiserade säkerhetsfunktioner i samtliga system.
D.6.10	E-post med höga skydds krav avseende konfidentialitet till extern mottagare ska krypteras. E-post med höga skydds krav enbart avseende riktighet ska kryptografiskt signeras men behöver inte krypteras.

D7. Anskaffning och utveckling av IT-resurser

Korrekt informationssäkerhet för IT-resurser ska säkerställas över hela livscykeln och börjar vid anskaffning eller utveckling. Örebro kommuns kravkatalog för IT-upphandling ska användas vid anskaffning, utveckling och upphandling av digitalt stöd.

Säkerhetskrav på IT-resurser

Krav som rör informationssäkerhet ska inkluderas i krav för nya IT-resurser och i krav för förbättringar av befintliga. Det gäller oavsett om IT-resursen upphandlas externt, utvecklas internt eller en kombination av båda (t.ex. anpassning av ett inköpt standardssystem).

Informationssäkerhetskrav ska baseras på branschstandarder, författningar och interna regelverk, riskanalyser eller analys av incidenter, samt spegla den klassning som tilldelats IT-resursen.

Utveckling, anskaffning eller förändring av system som omfattas av verksamhetsnära förvaltning ska involvera parterna i förvaltningsorganisationen. Objektägare IT ansvarar för att tekniska krav överensstämmer med verksamhetens krav, så att systemets skydd korrelerar med klassningen.

Utveckling, anskaffning eller förändring av underliggande IT-resurser i form av infrastruktur, stödsystem m.m. ska ha säkerhetskrav som minst motsvarande kraven på som de system som de stödjer. Ibland kan kraven däremot vara högre, exempelvis om en IT-resurs stödjer ett stort antal system med olika klassningsnivå.

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

Riktlinjer för säkerhetskrav på IT-resurser	
D.7.1	<p>Informationssäkerhet ska inkluderas i kraven för nya IT-resurser och i förändringar av befintliga. Det gäller oavsett om IT-resursen upphandlas externt, utvecklas internt eller en kombination av båda (t.ex. anpassning av ett inköpt standardssystem).</p> <p>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.</p>

Säkerhetskrav vid upphandling av IT-stöd

Vid upphandling av IT-stöd gäller ovanstående riktlinjer för säkerhetskrav på IT-resurser. Det är extra viktigt att vara tydlig i kravställning av informationssäkerhet vid en extern upphandling. Extern leverantör kan ha en annan förståelse för informationssäkerhet än vad vi har internt i kommunen. Exempelvis kan de ha en annan terminologi, tillämpa annan form för informationsklassning eller tolkar klassningsnivåerna på annat sätt.

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

I de fall som leverantör även ska ansvara för driften av upphandlat system så tillkommer krav. Se punkt D.7.6 nedan.

I kravspecifikationer ska alltid tydliga krav på säkerhet formuleras som sedan används vid utvärdering av anbud. Upphandling av IT-stöd ska alltid göras i samverkan med Örebro kommuns upphandlingsfunktion.

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 alltid 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 Örebro Kommun.
D.7.6	Upphandling av system med drift 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 kontinuitetshandling • Rätt till tredjepartsrevision • Sekretessförbindelse • Personuppgiftsbiträdesavtal • Rätt till incidentrapporter från leverantören
D.7.7	Upphandling av IT-stöd ska göras i samverkan med Örebro kommuns upphandlingsfunktion.
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 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 Örebro kommun genomför säkerhetstestning av system och ingående komponenter. • Att testet genomförs av tredje part. • Att leverantören ska åtgärda eventuella säkerhetsbrister som identifierats i samband med acceptanstest och/eller leveranskontroll.
D.7.10	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: <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

	<ul style="list-style-type: none"> • Vilka åtgärder som vidtas för att säkerställa att alla berörda parter, inklusive underleverantörer, är medvetna om sitt säkerhetsansvar, licensieringsarrangemang, äganderätt till koden och upphovsrätt • Vilka åtgärder som vidtas för att säkerställa kvalitet i leverans från underleverantör
--	--

Säkerhet vid systemutveckling

Processer och rutiner ska finnas på plats för att säkerställa att informationssäkerhet finns med under hela 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 kompetens i säker programutveckling. Med fördel kan utvecklingsprocesser innehålla utbildning och omvärldsbevakning.

Outsourcad systemutveckling ska övervakas och styras och säkerhetsfunktionalitet ska säkerställas. Leverantören ska använda en etablerad modell för utveckling av säker programvara. Dessa modeller kan användas i kravställningen runt utvecklingsprocesser beroende på vilken metod utvecklingsleverantören använder. Om ingen etablerad modell används av leverantören krävs en betydligt mer ingående analys för att säkerställa en säker utvecklingsprocess.

Riktlinjer för säkerhet 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 användning av Change management-processen.
D.7.13	För systemutvecklings- och integrationsåtgärder ska utveckling- och testmiljöer 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.

Säkerhetskrav vid test

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

Test med produktionsdata ska undvikas, men i annat fall ska personuppgifter anonymiseras. Testdata ska väljas ut noggrant, skyddas och kontrolleras, samt vara så lik produktionsdata som möjligt.

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

Driftsättning ska ske enligt Change management-processen.

Riktlinjer för säkerhetskrav vid test	
D.7.16	Säkerhetsfunktionalitet ska testas vid utveckling och testning ska göras gentemot de ställda säkerhetskraven, 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 styrs. 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 objektägare IT varje gång produktionsdata kopieras till ett testsystem • Produktionsdata ska omgående raderas från testsystem efter avslutad test • Kopiering av produktionsdata ska loggas för att erhålla spårbarhet.
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 Change management-processen.

D8. Informationssäkerhetsincidenter

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

Alla medarbetare i Örebro kommun är skyldiga att rapportera incidenter (se Kapitel A). Detta innefattar självklart även medarbetare på Informationsförsörjnings- och digitaliseringsavdelningen 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 Kommunsupport.

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 används 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 även 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 korrigerande och förebyggande åtgärder kan vidtas
- Återkoppling och kommunikation med dem som är påverkade av eller involverade i återhämtning efter incidenten liksom till den som rapporterat incidenten

Incident manager leder hanteringen av incidenter i samverkan med berörda ägare av objekt och 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.

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

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

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

Riktlinjer för incidenthantering	
D.8.1	Det ska finnas en process 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 korrigerande och förebyggande 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 IT-relaterade informationssäkerhetsincidenter ska sammanställas i rapporter som respektive objektägare ansvarar för att ta fram i samverkan med incident manager.
D.8.3	Erfarenheter från inträffade informationssäkerhetsincidenter 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	Informationssäkerhetsincidenter 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 informationssäkerhetsincident eller svaghet där brott misstänks föreligga, ska inte själva försöka bevisa detta då det kan försvåra utredningar.

Krisorganisation och krisplan

En krisplan ska finnas som ska aktiveras vid händelse av allvarliga incidenter eller i IT-miljön. Krisplanen ska ha en ansvarig förvaltare och innehålla bl.a. krisorganisation, kontaktpersoner och operativa steg att vidta under en allvarlig störning eller kris.

Riktlinjer för krisorganisation och krisplan	
D.8.6	Det ska finnas en krisorganisation på Informationsförsörjnings- och digitaliseringsavdelningen för allvarliga incidenter och kriser som tydligt beskriver roller och ansvar.
D.8.7	Det ska finnas en krisplan på Informationsförsörjnings- och digitaliseringsavdelningen som ska aktiveras vid händelse av en allvarlig incident eller kris. Krisplanen ska bl.a. innehålla krisorganisation, kontaktpersoner och operativa steg att vidta under en allvarlig störning eller kris.
D.8.8	Krisplanen ska testas och övas regelbundet. Identifierade brister och svagheter ska åtgärdas i syfte att ständigt förbättra krisplanen för Informationsförsörjnings- och digitaliseringsavdelningen.

D9. IT-relaterad kontinuitetshantering

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

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

Detta innebär att det måste finnas beredskap för hur man hanterar avbrott, s.k. avbrottsplaner, för IT-resurser med **höga skydds krav** avseende tillgänglighet. Objektägare IT ansvarar för att avbrottsplaner finns på plats och att de motsvarar de krav som finns för IT-resurserna. Avbrottsplaner ska vara relaterade till incidenthanteringen och den övergripande krisplan som ska finnas på Informationsförsörjnings- och digitaliseringsavdelningen (se avsnitt D8). En viktig säkerhetsåtgärd för att skapa och bibehålla hög tillgänglighet är säkerhetskopiering (se avsnitt D5).

Riktlinjer för kontinuitetshantering	
D.9.1	Det ska finnas avbrottsplaner för samtliga 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 innehåller planerna konfidentiell information och ska förvaras och hanteras förenligt med detta.

D10. Granskning och kontroll

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

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

Revision av hela eller stora delar av IT-miljön ska göras minst vartannat år, men kan även förekomma i samband med andra granskningar och revisioner kopplat till informationssäkerhet.

Riktlinjer för granskning och kontroll	
D.10.1	Kritiska delar i IT-miljön som stödjer objekt med höga skydds krav ska regelbundet övervakas och granskas för att sårbarheter och brister ska upptäckas.
D.10.2	Nya IT-lösningar ska vid minsta osäkerhet gällande säkerhetsförhållanden utsättas för tekniska granskningar av extern part (t.ex. penetrationstester).
D.10.3	Sårbarheter och brister som upptäcks vid granskningar ska tas upp för åtgärdande i objektplaner. Akuta sårbarheter och brister ska åtgärdas omedelbart.
D.10.4	Rapportering av större sårbarheter och brister ska ske till informationssäkerhetsrådet.
D.10.2	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 objektägare • Omfattningen av tekniska aktiviteter för granskning eller revision ska beskrivas för- och godkännas av IT-resursens ägare. • Aktiviteter vid granskning eller revision begränsas om möjligt till skrivskyddad åtkomst av program och data • Granskning som kan påverka tillgänglighet bör utföras under servicefönster eller vid sådan tidpunkt då påverkan på verksamheten är så liten som möjligt • All åtkomst vid granskning eller revision ska övervakas och loggas