Riktlinjer för informationssäkerhet i Alingsås kommun

Typ av styrdokument: Riktlinjer
Beslutande instans: Kommunstyrelsen
Datum för beslut: 2020-12-07, § 192
Diarienummer: 2020.525 KS

Gäller för: Kommunövergripande
Giltighetstid: Tillsvidare
Revideras senast: --
Dokumentansvarig: Informationssäkerhetssamordnare

ALINGSÅS
KOMMUN

Innehållsförteckning

Inledning

Alingsås kommuns informationssäkerhetspolicy innehåller kommunens viljeinriktning och övergripande principer avseende informationssäkerhetsarbetet i kommunen. Riktlinjer för informationssäkerhet konkretiserar informationssäkerhetspolicyn och innehåller mer detaljerad information och regler för hur information får hanteras i kommunen.

Detta dokument grundar sig på den vedertagna standardserien för informationssäkerhet, SS-ISO/IEC 27000.

Riktlinjernas omfattning

Riktlinjer för informationssäkerhet innehåller information och regler gällande säkerhet vid all hantering av information inom Alingsås kommun.

Riktlinjerna gäller för kommunens samtliga verksamheter, förutom de kommunala bolagen samt räddningstjänstförbund. Det finns inte utrymme att besluta om lokala regler som avviker från dessa riktlinjer.

Struktur och läsanvisningar

Dokumentet är uppdelat i fyra kapitel (A-D) vilka riktar sig till olika målgrupper.

Kapitel		Innehåll	Primär målgrupp	Sidor
A	Styrning av informationssäkerhet	Ansvarsfördelning för informationssäkerhet. Information och riktlinjer för hur arbetet med informationssäkerhet ska bedrivas.	Alla som arbetar med IT- och informationssäkerhet	xx
B	Informationssäkerhet för medarbetare	Information och riktlinjer för hur information och IT ska hanteras i olika situationer.	Alla medarbetare	xx
C	Informationssäkerhet i verksamhet och förvaltning	Information och riktlinjer för informationssäkerhet i förvaltningsobjekt som t.ex. system och grupper av system.	Informationsägare, systemägare	xx
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 IT-avdelningen	xx

Varje kapitel består av information och riktlinjer som är obligatoriska. Riktlinjerna är numrerade och i tabellform. Med konfidentiell information avses information som endast får vara tillgänglig för medarbetare som har särskild behörighet att hantera informationen, exempelvis sekretessbelagd information, känsliga personuppgifter, patientjournaler m.m. Denna typ av information kräver mer långtgående säkerhetsåtgärder och är markerad med dubbellinje.

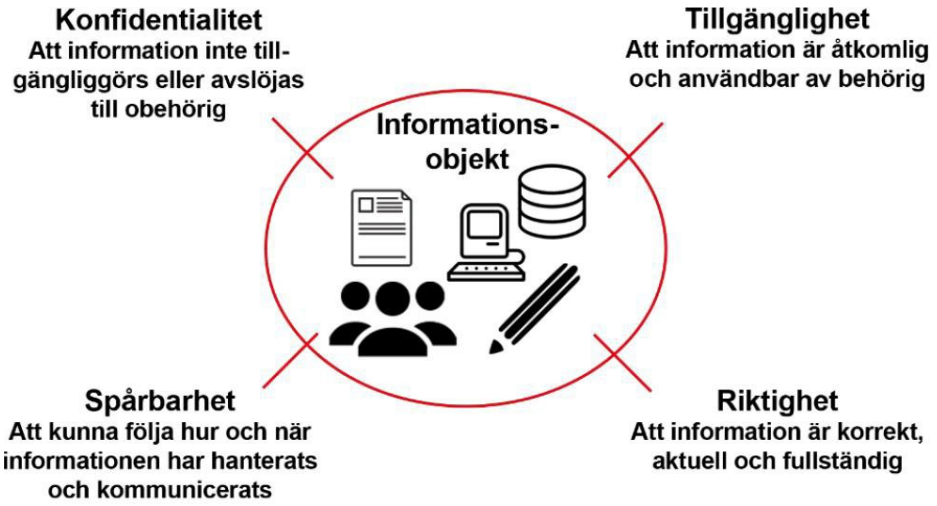
Riktlinjer för utformning av lösenord	
B.3.5	Enheter ska låsas med lösenord.
B.3.6	**Konfidentiell** information måste vara krypterad på mobila enheter.

Dispenser och undantag

Önskan om dispens och undantag från dessa riktlinjer ställs till kommunens informationssäkerhetssamordnare och IT-säkerhetssamordnare. Beslut om godkännande fattas av kommunens informationssäkerhetssamordnare och IT-säkerhetssamordnare i samråd med berörda.

Undantag och dispenser är inte permanenta utan ska ha en giltighetstid som bedöms från fall till fall. Efter att giltighetstiden passerat ska en ny begäran om dispens göras.

Om informationssäkerhet



Termer och definitioner

Term	Definition
Autentisering	Verifiering av att en användare eller IT-resurs är den som den utger sig för att vara.
Behandling av personuppgifter	Varje åtgärd eller serie av åtgärder som någon vidtar med personuppgifter, vare sig det görs på automatiserad väg eller inte.
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.
Hot	Möjlig oönskad händelse med negativa konsekvenser för verksamheten.
Information	Innebörd i data, d.v.s. data tolkad av människor.
Informationsklassning	Att genom klassificering identifiera skyddsbehovet för en viss informationsmängd.
Informationssäkerhet	Konfidentialitet, riktighet, tillgänglighet och spårbarhet hos information.
Informationssäkerhetsincident	En eller flera händelser som kan tänkas få allvarliga konsekvenser för verksamheten och hota informationssäkerheten
Informationssäkerhetspolicy	Organisationens viljeinriktning med informationssäkerhet uttryckt av dess 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.
Konfidentiell information	Information som endast får vara tillgänglig för medarbetare som har särskild behörighet att hantera informationen, exempelvis sekretessbelagd information, känsliga personuppgifter m.m
Känsliga personuppgifter	Uppgifter som avslöjar etniskt ursprung, politiska åsikter, religiös eller filosofisk övertygelse, medlemskap i fackförening, uppgifter som rör hälsa, sexualliv eller sexuell läggning samt genetiska och biometriska uppgifter. Patientuppgifter är känsliga uppgifter.
Ledningssystem för informationssäkerhet (LIS)	Ett administrativt ledningssystem som syftar till att upprätta, införa, driva, övervaka, granska, underhålla och förbättra organisationens informationssäkerhet.
Personuppgifter	All slags information som direkt eller indirekt kan knytas till en fysisk person som är i livet. Bild- och ljuduppgifter om en identifierbar fysisk person räknas som personuppgifter, även om inga namn nämns. Krypterade uppgifter och olika slag av elektroniska identiteter är också personuppgifter om de direkt eller indirekt kan kopplas till fysiska personer som är i livet.

Personuppgiftsansvarig	Personuppgiftsansvarig(PuA) är den som bestämmer för vilka ändamål uppgifterna ska behandlas och hur behandlingen ska gå till. Respektive nämnd och styrelse är personuppgiftsansvarig i en kommun
Riktighet	Att information är korrekt, aktuell och fullständig.
Risk	Produkten av sannolikheten och konsekvensen att ett hot realiseras.
Sekretess	Information som inte ska lämnas ut och bli allmänt tillgänglig. Sekretessbelagd uppgift innebär tystnadsplikt för den som har eller har fått befattning om uppgiften.
Spårbarhet	Entydig härledning av utförda aktiviteter till en identifierad användare eller IT-resurs.
Tillgänglighet	Att information är åtkomlig och användbar av behörig.

Kapitel A: Styrning av informationssäkerhet

Inledning

Detta kapitel beskriver och reglerar hur arbetet med informationssäkerhet ska bedrivas i Alingsås kommun. Målgruppen för detta kapitel är de som arbetar med informations- och IT-säkerhet eller har ansvar för informationssäkerhet.

A1. 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 informationssäkerhetssamordnare och övriga som arbetar specifikt med informationssäkerhet, IT-säkerhet eller andra relaterade frågor fungerar som stöd till medarbetare, verksamheter och kommunens ledning att kunna ta ansvaret för informationssäkerheten.

Övergripande ansvar

Kommunfullmäktige fastställer övergripande mål och principer för informationssäkerhetsarbetet genom en kommunövergripande informationssäkerhetspolicy.

Kommunstyrelsen ansvarar för att kommunens informationssäkerhetspolicy följs och för samordning av informationssäkerhetsarbetet i kommunen. Kommunstyrelsen ansvarar för utarbetning och fastställande av riktlinjer för informationssäkerhet.

Kommundirektören har ansvar för att informationssäkerhetsarbetet bedrivs i linje med den av fullmäktige fastställda informationssäkerhetspolicyn.

Ansvar inom respektive verksamhet

Varje nämnd/styrelse är ansvarig för informationssäkerheten inom sitt verksamhetsområde, informationssäkerhetsansvaret kan inte delegeras.

Nämnd/styrelse kan vid behov besluta om instruktioner som kompletterar de centrala riktlinjerna för informationssäkerhet.

Respektive förvaltningsledning ska säkerställa att medarbetare efterlever dessa riktlinjer. Vidare ska respektive förvaltningsledning säkerställa att medarbetare har ett säkerhetsmedvetande och tillräcklig förståelse och kunskap för att en erforderlig informationssäkerhet kan uppnås. Ansvaret omfattar även att tillgängliga tjänster/processer/system används på de sätt dom är avsedda.

Medarbetares ansvar

Den enskilde medarbetaren är ansvarig för att följa gällande bestämmelser kring informationssäkerhet. Varje medarbetare är skyldig att rapportera informationssäkerhetsrelaterade brister och incidenter.

Personuppgiftsansvar

Personuppgiftsansvarig har det yttersta ansvaret för all behandling av personuppgifter inom sitt verksamhetsområde. Kommunstyrelsen och övriga nämnder/bolag är personuppgiftsansvariga inom respektive verksamhetsområde och ska utse dataskyddsombud.

Kommunarkivet
Kommunarkivet har tillsynsansvar för att informationen hanteras enligt bestämmelserna i tryckfrihetsförordningen, arkivlagen och offentlighets- och sekretesslagen, samt kommunens interna styrdokument rörande informationens långsiktiga hantering och bevarande.

System-/Objektägares ansvar
System-/Objektägare ansvarar för att objekt efterlever informationssäkerhetspolicy och riktlinjer för informationssäkerhet. Informationssäkerhetsansvar hos övriga roller inom förvaltnings-organisationen beskrivs i Kapitel C.

Förvaltningschef är ytterst ansvarig för system/objekt inom sin verksamhet, förvaltningschef kan delegera system-/objektägarskap till annan roll inom sin verksamhet.

Ansvar i projekt
Utsedd projektägare säkerställer att säkerhetsfrågorna beaktas och ansvarar för fastställande av säkerhetsnivå i projektet. Projektledaren tillsammans med styrgrupp ansvarar för informationssäkerheten beaktas och efterlevs under hela projekttiden.

IT-avdelningens ansvar
IT-avdelningen ansvarar för säkerheten i kommunens IT-miljö. Att tjänster, processer, system, infrastruktur, verktyg etc. motsvarar verksamheters krav, legala krav samt informationssäkerhetspolicyn och riktlinjerna för informationssäkerhet.

IT-säkerhetssamordnare
Det ska finnas en utpekad IT-säkerhetssamordnare. Denne har det övergripande ansvaret att säkerställa säkerheten i Alingsås kommuns IT-miljö och är stödjande vid kravställning gentemot externa aktörer. Rollen IT-säkerhetsansvarig beskrivs utförligare i Kapitel D.

Informationssäkerhetssamordnare
Det ska finnas en utpekad informationssäkerhetssamordnare. Informationssäkerhetssamordnare leder och samordnar kommunens informationssäkerhetsarbete.

Informationssäkerhetssamordnare ansvarar för följande:

- att kommunens styrande dokument inom området är aktuella
- att utveckla och förvalta metoder, vägledningar och annat stödmaterial inom informationssäkerhetsområdet
- kompetensförsörjning och att öka informationssäkerhetsmedvetandet inom kommunen, t.ex. genom rådgivning och utbildning
- att stödja verksamheterna i frågor som rör informationssäkerhet
- kontroll och uppföljning av informationssäkerheten i kommunen
- omvärldsbevakning inom informationssäkerhetsområdet
- sammankallar kommunens informationssäkerhetsråd
- administrerar SKR:s KLASSA-verktyg
- Rapporterar läge och status gällande informationssäkerhet till kommunstyrelsen en gång per år. Oftare om särskilda skäl finns som exempelvis allvarliga incidenter, brister eller behov.

Informationssäkerhetsrådet består av informationssäkerhetssamordnare, IT-säkerhetssamordnare, kommunjurist. Andra funktioner såsom säkerhetschef eller dataskyddsombud kan bjudas in för hantering av enskilda frågor. Informationssäkerhetssamordnare är sammankallande.

Informationssäkerhetsrådet träffas ca 3-4 gånger per år och hanterar följande frågor:

- beslut om undantag från kommunens Riktlinjer för informationssäkerhet (godkännes av informationssamordnare och IT-säkerhetssamordnare i samråd med berörda)
- beredning av dokument, t.ex. styrande dokument, metoder och vägledningar
- remissinstans och rådgivare i relaterade frågor
- vara ett forum för erfarenhetsutbyte och omvärldsbevakning
- godkänna specifika säkerhetslösningar som t.ex. krypteringsmetoder

Kommunens revisorer

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

A2. Dokumentstruktur

Följande dokument reglerar Alingsås kommuns arbete med informationssäkerhet:

- Säkerhetspolicy
- Riktlinjer för säkerhets- och beredskapsarbete i Alingsås kommun
- Riktlinjer för säkerhetsskydd
- Informationssäkerhetspolicy
- Riktlinjer för informationssäkerhet
- Handlingsplan för informationssäkerhet
- Nulägesanalys för informationssäkerhet

Informationssäkerhetspolicy och Riktlinjer för informationssäkerhet riktar sig till alla medarbetare inom Alingsås kommun.

Handlingsplan för informationssäkerhet och Nulägesanalys för informationssäkerhet riktar sig främst till de som arbetar med styrning av informationssäkerhet i Alingsås kommun.

Modeller, metoder, vägledningar och andra stöddokument tas fram centralt för att stödja arbetet med informationssäkerhet.

Riktlinjer för dokumentstruktur för informationssäkerhet	
A.2.1	Alingsås kommuns informationssäkerhet ska analyseras i en Nulägesanalys för informationssäkerhet. 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.
A.2.2	Årliga handlingsplaner för informationssäkerhet ska tas fram baserade på nulägesanalysen.
A.2.3	Det ska finnas en för Alingsås kommun övergripande informationssäkerhetspolicy som uttrycker ledningens viljeinriktning med informationssäkerhet.
A.2.4	Det ska finnas kommunövergripande riktlinjer för informationssäkerhet som konkretiserar informationssäkerhetspolicyn och som riktar sig till relevanta målgrupper.
A.2.5	Det ska finnas modeller, metoder, vägledningar och andra stöddokument som stödjer olika gruppers efterlevnad av informationssäkerhetpolicyn och riktlinjerna för informationssäkerhet.

A3. Informationsklassning

Informationsklassning är en grundläggande komponent i informationssäkerhetsarbetet. Informationsklassning innebär att verksamheter klassar sina informationstillgångar utifrån interna och externa krav på konfidentialitet, riktighet, tillgänglighet och spårbarhet. Genom att klassa information kan verksamheter identifiera känslig och kritisk information och säkerställa att denna får lämpligt skydd, ibland också för att undvika att information får onödigt överskydd.

I den vägledande standarden SS-ISO/IEC 27002 rekommenderas att man ska ta fram en organisationsgemensam modell för informationsklassning. I Alingsås kommun används SKR:s modell KLASSA.

Med konfidentiell information avses information som endast får vara tillgänglig för medarbetare som har särskild behörighet att hantera informationen, exempelvis sekretessbelagd information, känsliga personuppgifter, patientjournaler m.m. Denna typ av information kräver mer långtgående säkerhetsåtgärder.

Riktlinjer för informationsklassning	
A.3.1	Alingsås kommun ska ha en gemensam modell för informationsklassning.
A.3.2	Alingsås kommuns modell för informationsklassning ska tillämpas för kravställning på informationssäkerhet. Information ska klassas i enlighet med modellen och krav på säkerhetsåtgärder ska kopplas till de olika nivåerna i klassningsmodellen.

A4. Ledningssystem för informationssäkerhet (LIS)

I Alingsås kommuns informationssäkerhetspolicy anges att kommunens informationssäkerhetsarbete ska vara systematiskt. Att det ska bygga på den vedertagna standardserien ISO/IEC 27000 med strävan att ett ledningssystem för informationssäkerhet integreras i kommunens styrning.
Ett systematiskt arbete med informationssäkerhet med ett LIS syftar i stort till att informationssäkerheten över tid anpassas efter interna och externa förutsättningar, och som därigenom upprätthåller en lämplig skyddsnivå över tid.

I Alingsås kommun har arbetet med att skapa ett LIS påbörjats i och med dessa riktlinjer. Att planera och införa ett LIS kommer dock att fortgå under de närmaste åren.

Riktlinjer för ledningssystem för informationssäkerhet (LIS)	
A.4.1	Alingsås kommun ska införa samt underhålla ett ledningssystem för informationssäkerhet.

A5. Personalsäkerhet

Alingsås kommuns personal hanterar dagligen information, manuellt eller med stöd av IT. Många funktioner kommer i kontakt med och hanterar kritisk och känslig information, därför är det viktigt att personalen får information och utbildning om informationssäkerhet.

Före och i samband med anställning

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

Lagsstiftningen om registerkontroll för skydd av barn och unga ska följas.

ID-kontroll ska ske vid anställning.

Kritiska tjänster kräver en förstärkt kontroll i form av kreditupplysning och kontroll i brottsregister. Exempel på kritiska tjänster är högre chefstjänster, säkerhetstjänster, eller för de som har åtkomst till känslig eller samhällsviktig information.

För befattningar som har betydelse för rikets säkerhet och omfattas av Säkerhetsskyddslagen (2018:585), ska det i anställningsförfarandet genomföras en säkerhetsprövning. Säkerhetsprövningen ska genomföras innan en person genom anställning eller på annat sätt deltar i verksamhet som har betydelse för rikets säkerhet. De befattningar som är aktuella framgår av Alingsås kommuns säkerhetsskyddsplan. Säkerhetsprövningen administreras av kommunledningskontoret säkerhetsenhet.

Alla bakgrundskontroller ska ta hänsyn till gällande lagstiftning rörande hantering av person-uppgifter.

Nyanställda ska informeras om ansvar och skyldigheter kopplade till informationssäkerhet och genomgå utbildning i informationssäkerhet.

Riktlinjer för personalsäkerhet före och i samband med anställning	
A.5.1	Bakgrundskontroll av sökande ska göras före anställning där sökandes meritförteckning verifieras.
A.5.2	Anställning av kritiska roller ska genomgå förstärkt kontroll i form av kreditupplysning och kontroll i brottsregister.
A.5.3	För befattningar som har betydelse för rikets säkerhet, och som omfattas av Säkerhetsskyddslagen (2018:585) ska det i anställningsförfarandet genomföras en säkerhetsprövning.
A.5.4	Nyanställda ska informeras om ansvar och skyldigheter kopplade till informationssäkerhet och genomgå utbildning i informationssäkerhet.

Under anställning

Medarbetare ska få lämplig utbildning för att kunna efterleva kommunens informationssäkerhetspolicy och riktlinjer för informationssäkerhet. Detta gäller även externa aktörer såsom exempelvis konsulter. Medarbetare ska årligen genomgå utbildning i informationssäkerhet.

Roller som har särskilda uppgifter inom informationssäkerhet, t.ex. inom IT-säkerhet eller förvaltningsorganisationen, ska få lämplig fortbildning inom området som är relevant för respektive befattning.

Om anställda bryter mot gällande informationssäkerhetsregler ska dessa ärenden hanteras på samma sätt som vid andra misskötselärenden.

Riktlinjer för personalsäkerhet under anställning	
A.5.6	Samtliga medarbetare ska få lämplig utbildning för att kunna efterleva kommunens informationssäkerhetspolicy och riktlinjer för informationssäkerhet. Detta gäller även externa aktörer såsom exempelvis konsulter. Samtliga medarbetare ska årligen genomgå utbildning i informationssäkerhet.
A.5.7	Roller som har särskilda uppgifter inom informationssäkerhet ska får lämplig fortbildning inom området som är relevant för deras befattning.
A.5.8	Om anställda bryter mot gällande informationssäkerhetsregler ska dessa ärenden hanteras på samma sätt som vid andra misskötselärenden.

Avslut eller ändring av anställning

Vid avslut eller ändring av anställning kan ansvar och skyldigheter för informationssäkerhet fortsätta att gälla, exempelvis tystnadsplikt om den anställde haft tillgång till konfidentiell information. Chef ansvarar för att detta kommuniceras till den anställde vid anställning/tillträdande av roll.

Vid avslut eller ändring av anställning ska åtkomsträttigheter till information upphöra och återlämning av IT-resurser ske omgående.

Avlämnande chef ansvarar för att detta verkställs.

Riktlinjer för avslut eller ändring av anställning	
A.5.9	Ansvar och skyldigheter för informationssäkerhet som förblir gällande efter avslut eller ändring av anställning ska definieras och kommuniceras vid anställningstillfället av ansvarig chef.
A.5.10	Vid avslut eller ändring av anställning ska åtkomsträttigheter till information upphöra och återlämning av IT-resurser ske omgående.

A6. Efterlevnad och granskning

Årligen ska efterlevnad gällande de styrande dokumenten Informationssäkerhetspolicy och Riktlinjer för informationssäkerhet följas upp. Internkontroll

Revision av hela eller stora delar av Alingsås kommuns informationssäkerhet ska göras minst vartannat år.

Granskning av efterlevnad av informationssäkerhet bör också genomföras av extern part, exempelvis på uppdrag av kommunrevisionen.

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

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	
A.6.1	Årligen ska efterlevnad gällande de styrande dokumenten Informationssäkerhetspolicy och Riktlinjer för informationssäkerhet följas upp.
A.6.2	Alingsås kommuns informationssäkerhet ska utsättas för oberoende extern granskning.

Kapitel B: Informationssäkerhet för medarbetare

Inledning

Detta kapitel vänder sig till alla medarbetare vid Alingsås kommun. Riktlinjerna gäller även extern personal som har åtkomst till Alingsås kommuns information, exempelvis inhyrda konsulter.

Riktlinjerna beskriver en medarbetares ansvar vid hantering av information i Alingsås kommun och vilka regler som gäller. Kompletterande regler kan finnas lokalt då kommunen är en stor organisation med många skilda verksamheter. Dock får inte avvikelser ske från dessa riktlinjer utan tillstånd. Kontakta ansvarig chef vid osäkerhet om vad som gäller.

Medarbetares ansvar för informationssäkerhet

Information är en viktig resurs för Alingsås kommun och är av stor betydelse för alla kommunala verksamheter. Varje dag hanteras mängder av information som handlar om allt vi gör, exempelvis hemvård, socialtjänst, förskolor, grundskolor, gymnasium, bygglov, stadsplanering m.m. Information kan förekomma i olika former, muntlig, skriftlig eller finnas i IT-system. Informationens form kan vara i text, bild, symbol, film, geodata och ljud.

Kommunen ska uppfylla lagar och regler kring informationssäkerhet, likaså uppfylla och motsvara privatpersoners, företags och andra organisationers förväntningar och behov kring att kommunen hanterar information på ett säkert sätt. Medarbetares kunskap och medvetenhet kring informationssäkerhet utgör en viktig del av kommunens informationssäkerhetsarbete.

Om du bryter mot riktlinjer för informationssäkerhet följer Alingsås kommun reglerna enligt lagar och avtal för informationssäkerhet, misskötselärenden hanteras enligt kommunens ordinarie hantering.

Skyldighet att rapportera incidenter och brister

Samtliga medarbetare har skyldighet att rapportera incidenter eller brister som misstänks kunna medföra negativ påverkan på Alingsås kommuns information. Exempelvis phisingattacker, IT-angrepp/intrång, oskyddad känslig information, brister i efterlevnad av dessa riktlinjer för informationssäkerhet. Incidenter och brister ska rapporteras till Helpdesk och/eller närmaste chef. Beroende på incidentens art gör chef bedömning om vidare eskalering av frågan.

B1. Säkert beteende

Oavsett om du hanterar information digitalt, muntligt eller i pappersform, är din egen informationssäkerhet beroende av ditt beteende. Ett första steg mot ett säkrare beteende är att skaffa sig kunskap om risker och om informationens värde.

Ett säkert beteende kan exempelvis handla om att aldrig lämna ut koder eller lösenord, att inte lämna ut personliga uppgifter utan att vara säker på mottagarens avsikter, att låsa datorn då du lämnar din arbetsplats eller att tänka på vad man pratar om i mobiltelefonen då man åker kollektivtrafik. Särskilt försiktig behöver du vara vid hanteringen av konfidentiell information.
Med konfidentiell information avses information som endast får vara tillgänglig för medarbetare som har särskild behörighet att hantera informationen, exempelvis sekretessbelagd information, känsliga personuppgifter, patientjournaler m.m

Riktlinjer för muntlig information	
B.1.1	**Konfidentiell** information har en begränsad krets av behöriga. Detta måste beaktas så att inte obehöriga kan höra sådan information på arbetsplatsen, både i arbetssituationer men även i informella sammanhang, t.ex. vid fikabordet. Man ska enbart tala i stängda utrymmen och även försäkra sig om att fysiska samtal eller telefonsamtal inte hörs i intilliggande rum.
B.1.2	Endast öppen information ska kommuniceras hörbart utanför arbetsplatsen, exempelvis vid fysiska samtal på tåget, eller i telefonsamtal i kassakön. **Konfidentiell** information får överhuvudtaget inte kommuniceras muntligt i publika lokaler.

Riktlinjer för information på skärmar och i pappersform	
B.1.3	Skriftligt material som innehåller **konfidentiell** information får inte ligga framme så att obehöriga kan läsa den. Materialet ska låsas in i godkända skåp när man lämnar arbetsplatsen, även för kortare stunder.
B.1.4	**Konfidentiell** information på datorskärmen ska vara skyddad från obehöriga. Skärmen ska låsas när man lämnar datorn, även för en kortare stund.
B.1.5	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 hjälpas tillrätta.
B.1.6	Vid fysisk posttjänst ska förslutna brev användas för intern information och rekommenderade försändelser ska användas om brev innehåller **konfidentiell** information.
B.1.7	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.
B.1.8	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.
B.1.9	Pappersdokument som innehåller **konfidentiell** information måste vid kassering strimlas eller kastas i godkända säkerhetskärl.

B2. Lösenord

För inloggning i Alingsås kommuns IT-system används användar-ID och lösenord. Lösenorden är personliga och ska inte göras kända för andra. Får obehörig tillgång till ditt lösenord och användar-ID kan personen utföra aktiviteter i ditt namn.

Du får en notis om byte av lösenord vid inloggning till din dator.

För att skydda intern eller konfidentiell information används användar-ID och lösenord, därför är det av vikt att följa nedanstående riktlinjer för skapande och hantering av lösenord. Ett lösenord ska vara ”starkt”, det vill säga svårt att gissa för någon annan.

Vid behov kan enskilda riktlinjer gälla för verksamhetskritiska system.

Riktlinjer för utformning av lösenord	
B.2.1	Lösenord ska vara minst 8 tecken långt, gärna längre.
B.2.2	Lösenord ska innehålla minst en gemen, en versal och en siffra.
B.2.3	Tre generationer av användares tidigare lösenord sparas så att de måste använda ett nytt, unikt, lösenord när de ändrar.
B.2.4	Lösenord ska bytas efter 90 dagar om inte annat anges.

Riktlinjer för hantering av lösenord	
B.2.5	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.
B.2.6	Samma lösenord ska inte användas privat och i jobbet. Olika lösenord ska användas för olika tjänster på webben även om de är jobbrelaterade. På så vis minskas riskerna att någon kommer åt information.
B.2.7	Lösenord ska bytas regelbundet. Var 90:e dag tvingas användare till byte av lösenord till sitt användarkonto. Om man arbetar i system där lösenordsbyte inte är tvingande, ska man ändå byta ut lösenordet några gånger om året. Lösenord ska bytas direkt om misstanke finns att det har röjts.
B.2.8	Lösenord får inte delas. Lösenord är personliga och ska inte delas mellan kollegor. Man kan i så fall bli ansvarig för något som någon annan har gjort. I de fall en dator delas av flera, ska ändå personliga inloggningar göras. Detta är viktigt för spårbarheten, för att kunna veta vem som har gjort vad i systemen.
B.2.9	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.
B.2.10	Användarkonto låses efter fem misslyckade inloggningsförsök.

B3. Enheter

IT-utrustning som tillhandahålls av Alingsås kommun kan vara stationär eller mobil. Med mobil enhet menas bärbar dator (laptop), USB-minne, CD/DVD-skiva, extern hårddisk, smart telefon och surfplatta. Applikationsspecifika datorer, mobiler eller surfplattor, kan ha specifika riktlinjer utöver dessa som presenteras här.

Riktlinjer för hantering av enheter	
B.3.1	Enheter som tillhandahålls av Alingsås kommun är personliga arbetsredskap och får inte lånas eller överlåtas om det inte är enheter som delas av flera.
B.3.2	Uppsatta säkerhetsinställningar i enheter får inte ändras.
B.3.3	Endast godkända programvaror får installeras på enheten.
B.3.4	Installerad programvara får inte kopieras eller installeras på annan enhet.
B.3.5	Enheter ska låsas med lösenord.
B.3.6	**Konfidentiell** information måste vara krypterad på mobila enheter.
B.3.7	Viktig information bör inte lagras enbart på en bärbar enhet, i så fall ska den snarast kopieras över till kommunens nätverk så att informationen säkerhetskopieras.
B.3.8	Endast av kommunen godkänd enhet och programvara får anslutas till kommunens nät.
B.3.9	Privat utrustning kan anslutas till kommunens gästnät.
B.3.10	Enheten får enbart anslutas till trådlösa nätverk som är kända och lösenordskyddade.
B.3.11	Vid distansarbete måste godkänd säker utrustning och anslutning användas.
B.3.12	Anslutning med kommunens VPN-anslutning från en privat dator är ej tillåtet.

Riktlinjer för fysisk hantering av enheter	
B.3.13	Försiktighet ska iakttas vid arbete i publika miljöer, exempelvis kan skärmen skyddas med sekretesskydd.
B.3.14	Arbete med **konfidentiell** information får inte ske i publika miljöer.
B.3.15	Enheter får inte lämnas utan uppsikt och ska förvaras i säkert och skyddat utrymme.
B.3.16	Förlust av enhet ska omedelbart anmälas till Helpdesk, detta ska göras innan polisanmälan om så är möjligt. I vissa fall finns möjligheter att fjärradera information.
B.3.17	Vid avslut av anställning eller vid byte till en annan enhet ska enheter återlämnas i enlighet med de rutiner som finns, och får inte behållas privat eller av en verksamhet.
B.3.18	Utrustningen ska i övrigt vårdas och hanteras på det sätt som föreskrivs, t.ex. skyddas mot värme och fukt.

Särskilda regler för smarta telefoner och surfplattor

Tillsammans med de regler som gäller allmänt för enheter gäller även följande vid användning av smarta telefoner och surfplattor:

Regler för smarta telefoner och surfplattor	
B.3.19	Alingsås kommun som arbetsgivare äger de smarta telefoner och surfplattor som används i tjänsten och även 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.
B.3.20	Det finns ett stort utbud av appar att ladda ner till den smarta telefonen eller surfplattan. Många appar kan innehålla skadlig kod. För att minska denna risk är det endast tillåtet att ladda ned appar från godkända distributörer. Avvikelser för specifika verksamheter kan förekomma.
B.3.21	Information som är **konfidentiell** får inte hanteras i smart telefon eller surfplatta om inte särskild av kommunen godkänd säkerhetslösning används.
B.3.22	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.
B.3.23	Vårda utrustningen och använd exempelvis skärmskydd och skal.

B4. Skadlig kod

Skadlig kod är ett samlingsnamn för olika typer av programvaror som orsakar avsiktlig störning eller skada. I begreppet skadlig kod ingår bland annat virus, maskar, trojaner, exploits och rootkits. Skadlig kod är ett växande problem vilket blir mer och mer sofistikerad och ”intelligent”.

Spridning av skadlig kod

Skadlig kod kan på olika sätt spridas till ens dator eller mobila enhet, exempelvis om man öppnar bilagor i e-post, importerar filer eller klickar på fel länkar.

Vid Phishing luras mottagaren att klicka på en länk som leder till en sida där man ombeds fylla i koder, lösenord eller bankkonton. Var observant på detta och fyll aldrig i sådana uppgifter.

Blir IT-utrustning drabbat av skadlig kod och kopplas upp i kommunens nätverk kan det spridas vidare i nätverket och orsaka stor skada.

Alingsås kommuns enheter är utrustade med skydd mot skadlig kod. Detta innebär inte fullständig säkerhet då utvecklingen inom detta område går snabbt.

Riktlinjer för skydd mot skadlig kod	
B.4.1	Stäng aldrig av eller på annat sätt inaktivera installerat skydd mot skadlig kod.
B.4.2	Anslut endast godkänd IT-utrustning till kommunens nätverk.
B.4.3	Var misstänksam och undvik att klicka på konstiga länkar. Lämna aldrig ut användarID eller lösenord.
B.4.4	Öppna bifogade filer endast om de kommer från en känd avsändare och en bilaga är förväntad.
B.4.5	Var observant på om IT-utrustning beter sig långsamt eller konstigt. Vid misstanke om skadlig kod kontakta Helpdesk.

B5. Internet och sociala medier

Förutom de riktlinjer i avsnitt B4 som är kopplade till skadlig kod följer särskilda regler för användning av Internet och sociala medier:

Riktlinjer för Internetanvändning	
B.5.1	Internet är i arbetet på Alingsås kommun främst ett arbetsverktyg och ska inte störa ordinarie arbetsuppgifter eller innebära merkostnader för kommunen.
B.5.2	De regler som gäller i samhället i övrigt gäller självklart även inom Alingsås kommun. Tryckfrihetsförordningen, brottsbalken, lagen om upphovsrätt samt dataskyddsförordningen är exempel på lagar som ibland måste beaktas när man använder Internet.
B.5.3	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.
B.5.4	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, Alingsås kommuns nätverk.
B.5.5	Internet är ett öppet nätverk och endast öppen information får publiceras eller delas, alltså inte **konfidentiell** information.

Det är av vikt att som representant för Alingsås kommun beakta god etik och gott omdöme på Internet. Alingsås kommuns etiska regler och värderingar ska följas även vid kommunikation via Internet och sociala medier. Tänk därför på att:

Etiska riktlinjer	
B.5.6	All kommunikation på Internet från Alingsås kommuns datorer ska vara öppen, saklig och etisk, oavsett om kommunikationen sker för privata syften eller inte.
B.5.7	Det är inte tillåtet att besöka webbplatser med till exempel brottslig verksamhet, rasism, diskriminering, extrempolitiskt eller pornografiskt innehåll.
B.5.8	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 noga innan du publicerar.

Riktlinjer vid användning av sociala medier	
B.5.9	Vid användning av sociala medier, se till så att det inte framstår som om åsikter som uttrycks är Alingsås kommuns.
B.5.10	Då du använder sociala medier privat, så kan kopplingar göras till din arbetsgivare.

Mer information om användning av sociala medier finns i Alingsås kommuns riktlinjer för sociala medier

B6. E-post

För många medarbetare är e-post det vanligaste och viktigaste sättet att kommunicera såväl internt som externt. Det är viktigt att tänka på att kommunikation med e-post inte är en fullt säker kommunikationsväg. Då vi inte kan säkerställa vidare distribution och mottagare av information.

Ansvar	
B.6.1	Den enskilde medarbetaren som är kontoinnehavare för ett personligt e-postkonto är alltid ansvarig för den e-post som skickas från kontot.
B.6.2	Medarbetare är ansvarig för att löpande öppna och läsa inkommande e-post. Vid frånvaro, t.ex. semester, sjukfrånvaro eller föräldraledighet, ska autosvar användas, och om nödvändigt hänvisning till kollega eller chef. Vid avslut av anställning eller vid tjänstledighet tas e-posten bort.
B.6.3	E-postkonton som delas av flera, t.ex. myndighetsbrevlådor/funktionsbrevlådor ska ha utpekade ansvariga.

Allmänna handlingar	
B.6.4	E-post som skickas till personliga brevlådor är allmän handling om innehållet är arbetsrelaterat. Vid arbetsrelaterad e-post ska alltid regler för registrering och hantering av allmänna handlingar följas. Huvudregeln är att e-post som är allmän handling omgående ska vidarebefordras till registrator.
B.6.5	E-post som är allmän handling får gallras, dvs. raderas. Gallring sker i enlighet med respektive dokumenhanteringsplan.

Privat e-post	
B.6.6	Håll isär arbetsrelaterad och privat kommunikation när du kommunicerar via e-post. Använd privat e-postadress för privat kommunikation.
B.6.7	Det är inte tillåtet att automatiskt vidarebefordra e-post till externa e-postadresser.

E-post och konfidentiell information	
B.6.8	Öppen och intern information får skickas med e-post, medan **konfidentiell** information endast får skickas med e-post som använder av Alingsås kommun godkänd kryptering.
B.6.9	Dokument som skannas skickas ofta med e-post från skannern till mottagarens e-postadress. Skanning av dokument som innehåller **konfidentiell** information ska även den krypteras av Alingsås kommun godkänd kryptering.

B7. Lagring och säkerhetskopiering

Information ska lagras på ett säkert sätt och säkerhetskopieras så att den kan återskapas i händelse av diskkrasch, oavsiktlig radering m.m.

Riktlinjer för lagring och säkerhetskopiering	
B.7.1	Information ska lagras på gemensamma lagringsytor(ex Alfresco, G:) i nätverket så att den säkerhetskopieras.
B.7.2	Om information behöver lagras på lokal hårddisk, se till att regelbundet kopiera över informationen till nätverket.
B.7.3	Om information har gått förlorad, exempelvis om man av misstag råkat radera ett dokument, ska Helpdesk kontaktas, förhoppningsvis kan de då återskapa den senaste säkerhetskopian.
B.7.4	**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.
B.7.5	Lokal lagring av **konfidentiell** information, t.ex. på en persondator, får endast ske om lagringsenheten eller filerna är krypterade av Alingsås kommun godkänd metod för kryptering.
B.7.6	Fysiska dokument som innehåller **konfidentiell** information ska förvaras inlåsta.

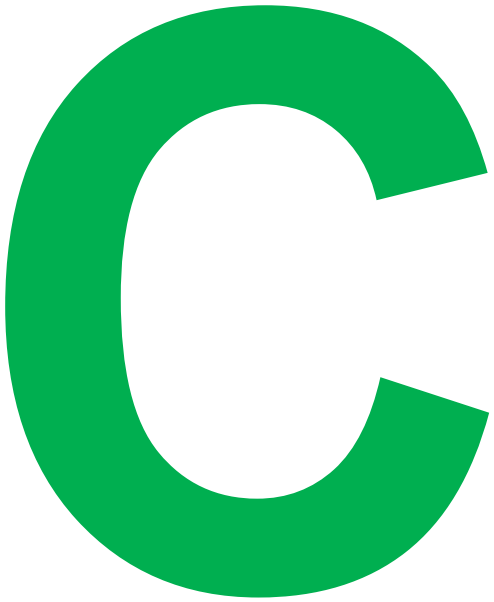
Molntjänster är datortjänster som tillhandahålls över Internet, exempelvis lagring eller programvaror.

Riktlinjer för lagring i molntjänster	
B.7.7	Endast godkända molntjänster är tillåtna att användas. Kontrollera vilka molntjänster som är tillåtna inom din verksamhet.
B.7.8	**Konfidentiell** information får inte lagras i personliga molntjänster.

B8. Spårbarhet och loggning

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

Vid misstanke om brott har Alingsås kommun 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.



Kapitel C: Informationssäkerhet i verksamhet

Inledning

Det här kapitlet innehåller riktlinjer kopplat till verksamhetsnära förvaltning och riktar sig främst till roller i denna.
För varje system eller objekt ska det upprättas en systemförvaltningsplan för att säkerställa drift och tillämpning av riktlinjerna för informationssäkerhet. Det ska finnas en utsedd ägare för varje system som ansvarar för säkerheten i systemet.

Roller och ansvar

Ansvaret för informationssäkerhet följer verksamhetsansvaret, från kommunledningen till den enskilde medarbetaren. Detta innebär att den som är ansvarig för en viss verksamhet också är ansvarig för informationssäkerheten inom verksamhetsområdet. Informationssäkerhetsamordnare och övriga som jobbar specifikt med informationssäkerhet fungerar som stöd till kommunens verksamheter att uppfylla informationssäkerhetsansvaret.

Ledning, kommunfullmäktige, kommunstyrelse och nämnder har det yttersta ansvaret för informationssäkerheten i den verksamhet som bedrivs inom respektive ansvarsområde.

Förvaltningschef ansvarar för informationssäkerheten inom sin verksamhet. Förvaltningschef ansvarar för att medarbetare inom den egna verksamheten har ett säkerhetsmedvetande samt tillräcklig kunskap och förståelse för att nödvändig informationssäkerhet i verksamheten ska uppnås.

System- eller objektägare ansvarar för att system eller objekt efterlever policy och riktlinjer för informationssäkerhet.

Systemförvaltare, ansvarar för att tillsammans med systemägaren upprätta systemförvaltningsplan och säkerställa efterlevnaden av upprättad plan. Det senare handlar bland annat om att informationssäkerhetsrelaterade mål och åtgärder nås samt genomförs.

C1. Dokumentation av informationssäkerhet

Informationssäkerhet ska vara en naturlig del i förvaltningen av objekt och system som kommunen använder. Det ska finnas systemdokumentation för varje IT-system. Dokumentationen består av systemförvaltningsplan, systemsäkerhetsbeskrivning, drift- och användardokumentation. Systemägaren ansvarar för att systemdokumentation tas fram och hålls aktuell.

Riktlinjer för dokumentation av informationssäkerhet	
C.1.1	Det ska finnas systemdokumentation för varje IT-system. Dokumentationen består av systemförvaltningsplan, systemsäkerhetsbeskrivning, drift- och användardokumentation.

C2. Informationsklassning och systemklassning

Informationsklassning innebär att information klassificeras i olika nivåer utifrån dess skyddskrav. Genom att klassa information på detta sätt kan man identifiera känslig och kritisk information så att denna får lämpligt skydd, men ibland också för att undvika att information får onödigt överskydd.

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

Klassning av information och system ska ske i SKR:s verktyg KLASSA. Verktyget ska identifiera verksamhetens behov av tekniska och administrativa säkerhets- och skyddsåtgärder för informationen. Verktyget används för att värdera informationen i kommunens system och genererar handlingsplaner som identifierar en del av de åtgärder som behöver vidtas för att uppfylla beslutad säkerhetsnivå.

Riktlinjer för klassning av system och objekt	
C.2.1	Data eller information i system eller objekt ska vara inventerad och klassad enligt SKR:s modell för informationsklassning.

C3. Behörighetshantering och loggning

Behörigheter, eller åtkomsträttigheter, anger vad en användare har rätt att utföra, t.ex. läsa, söka, skriva, radera, skapa eller köra ett program.

För att skydda information mot obehörig åtkomst behöver användare ange en identitet som kan verifieras (autentiseras), vanligen med användar-ID och lösenord. Desto känsligare och skyddsvärd information som bearbetas, desto högre är kravet på skydd mot obehörig åtkomst.

Behörighetstilldelning

Behörigheter ska tilldelas utifrån vad som behövs för att utföra tilldelade arbetsuppgifter.

Ansvar för behörighetstilldelning

Ansvarig chef bestämmer vilka roller som ska få tillgång till system/objekt och vilka behörigheter dessa ska ha. För externa användare gäller att tilldelning av åtkomst även ska vara tidsbegränsad för den tiden som behövs för att utföra uppgiften. Systemägare/Objektägare ansvarar för att detta verkställs.

Varje användare ska ha ett unikt Användar-ID, dvs. gruppidentiteter är inte tillåtna (under vissa förutsättningar kan dock detta beviljas, se information under D.2.14).

Rutiner för behörighetsförvaltning och revision
Rutiner ska fastställas för hur beställning, registrering, ändring och avregistrering av behörigheter ska göras. Ansvarig chef ska godkänna medarbetares behörighet med nödvändig spårbarhet för uppföljning och kontroll. Åtkomst med utvidgade behörigheter , administratörsbehörigheter, ska begränsas till så få personer som möjligt.

Stark autentisering ska finnas för åtkomst till system som innehåller information med höga skyddskrav avseende konfidentialitet och riktighet. Rutiner för behörighetshantering ska följas upp och dokumenteras.

Logghantering
För att erhålla spårbarhet bör system övervakas och loggas avseende användaraktiviteter, avvikelser, fel och informationssäkerhetshändelser. Detta är särskilt viktigt, och obligatoriskt, om system hanterar information med höga skyddskrav.

När loggning används ska det finnas rutiner för dess hantering. Där ska framgå hur loggning går till, hur loggar skyddas mot manipulation och obehörig åtkomst, hur länge de sparas och hur de granskas.

Rutiner för loggning ska följas upp och dokumenteras.

Riktlinjer för behörighetshantering och loggning	
C.3.1	Det ska finnas dokumenterade 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 ska vara tidsbegränsad samt föregås av sekretessavtal.
C.3.4	Det ska finnas dokumenterade rutiner för logghantering i system/objekt.
C.3.5	**Höga skyddskrav** på konfidentialitet, riktighet eller tillgänglighet innebär också höga krav på spårbarhet. Loggning av användares aktiviteter i sådana system är obligatorisk.
C.3.6	Förändringar i anställningar och roller ska omedelbart rapporteras till ansvarig objekt/systemägare så att reglering av behörigheter kan ske.
C.3.7	Uppföljning ska ske av behörighetshantering och logghantering i system/objekt.

C4. Ändringshantering

Ändringar i system ska ske på ett strukturerat sätt för att säkra systemets säkerhet, funktionalitet och användbarhet och för att minimera antalet fel orsakade av förändringen.

Ändringar i system ska vara samordnade med ändringshanteringsprocessen inom den IT- nära förvaltningen. I Kapitel D som riktar sig till den IT-nära förvaltningen finns riktlinjer som rör bl.a. systemtest och hantering av testdata (avsnitt D7 – Anskaffning och utveckling av IT-resurser).

Avveckling av system ska ske på ett strukturerat sätt och i samråd med kommunarkivet så att information hanteras i enlighet med dokumenthanteringsplan och gällande arkivlagstiftning.

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

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 dokumenthanteringsplan).

C5. Användarinstruktioner

Systemägare/Objektägare ansvarar för att det finns användarinstruktioner till ett system. Användare ska ges utbildning enligt instruktionerna och kontroll ska göras att instruktionerna efterlevs. Användarinstruktionerna ska omfatta följande delar inom informationssäkerhet:

- Regler kring inloggning och lösenordshantering
- Behörigheter
- Särskilda instruktioner för hur **konfidentiell** information får hanteras, t.ex. känsliga eller skyddade personuppgifter
- Information om vad som loggas och konsekvenser av att bryta mot användar-instruktioner, 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

Riktlinjer för användarinstruktioner	
C.5.1	Informationssäkerhetsregler ska finnas med i användarinstruktioner alternativt hänvisas till.
C.5.2	Det ska finnas särskilda instruktioner för hantering av **konfidentiell** information som t.ex. skyddade personuppgifter.

C6. Risk- och sårbarhetsanalyser

En risk- och sårbarhetsanalys är en metodisk process som identifierar säkerhetsrisker och bestämmer dess betydelse.

En risk- och sårbarhetsanalys ska genomföras vid anskaffning av system/tjänst/verktyg, större förändringar, större systemuppdateringar, nyutveckling, nya användargrupper eller extern åtkomst. Det kan också vara förändringar utanför själva systemet eller dess kontroll som motiverar en risk- och sårbarhetsanalys, exempelvis ägarbyte av en systemleverantör eller en omorganisation som berör den verksamhet som systemet stödjer. Alingsås kommuns grundmetod för risk- och sårbarhetsanalys ska användas resultat ska dokumenteras. En risk- och sårbarhetsanalys kan leda till åtgärdsbehov som behöver genomföras omedelbart eller på lite längre sikt och kan då tas med i kommande systemförvaltningsplan.

Riktlinjer för risk- och sårbarhetsanalyser	
C.6.1	Risk- och sårbarhetsanalys ska genomföras i samband med större förändringar i eller omkring system/processer.
C.6.2	Resultat ska dokumenteras. Akuta risker ska tas om hand skyndsamt och återstående åtgärder ska tas med i systemförvaltningsplaner.

C7. Incidenthantering

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

Mindre incidenter kan vara 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.

Allvarliga incidenter är större störningar i ett system som t.ex. ett längre uppehåll, dataintrång eller infektion av skadlig kod. En allvarlig incident kräver en utredning där dokumentation ska göras enligt gällande mall för allvarliga IT-relaterade incidenter, detta görs i samråd med IT-avdelningen.

Flera fall av mindre incidenter av likadan art kan tillsammans utmynna i eller utgöra en allvarlig incident.

Systemägare ska årligen sammanställa allvarliga incidenter som är kopplade till systemet. Kvarstående åtgärdsbehov som inträffade incidenter medfört ska tas om hand i systemförvaltningsplaner.

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 enligt gällande mall.
C.7.5	Allvarliga incidenter som rör system ska dokumenteras och sammanställas. Kvarstående åtgärdsbehov ska tas om hand i systemförvaltningsplaner.

C8. Kontinuitetshantering

Verksamheten ska kunna fortsätta även om till exempel IT-system slås ut, en strömkabel grävs av eller byggnader brinner ner. Krav på säkerställd drift gällande system och processer identifieras genom informationsklassning. Dvs att skyddsnivå för systemets tillgänglighet fastslås. Höga skyddskrav för tillgänglighet innebär högre krav på säkerhetskopiering och redundans.

Oavsett vilka säkerhetsåtgärder som valts kan avbrott ändå ske. System kan för verksamheten vara av så avgörande vikt att systemet 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 nyckelpersonal ska nyckelpersonberoendet åtgärdas t.ex. genom utbildning av ersättare och systemdokumentation.

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

Kapitel D: Informationssäkerhet i IT-miljön

Inledning

Kapitel D handlar om säkerhet i Alingsås kommuns IT-miljö. Riktlinjerna vänder sig främst till chef och medarbetare inom Alingsås kommuns IT-avdelning. Därtill externa parter som arbetar på uppdrag åt Alingsås 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.

Roller och Ansvar

Ansvar för informationssäkerhet och IT-säkerhet inom IT-avdelningen följer ordinarie verksamhetsansvar. Det innebär att chef och medarbetare inom respektive ansvarsområde ansvarar för att upprätthålla rätt nivå av informations- och IT-säkerhet för de processer och de IT-resurser de ansvarar för. IT-chef är ytterst ansvarig för att säkerställa säkerheten i Alingsås kommuns IT-miljö.

IT-säkerhetsansvarig

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

För den IT-säkerhetsansvarige innebär detta i huvudsak att:

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

Den IT-säkerhetsansvarige arbetar nära kommunens informationssäkerhetsansvarige och ingår i Alingsås kommuns informationssäkerhetsråd. Den IT-säkerhetsansvarige ska också omvärlds- bevaka, nätverka och samverka externt inom området med exempelvis MSB, cert.se, SIG Security, SKR och andra kommuner.

Roller i den IT-nära förvaltningen

Objekt/system-ägare IT

Objekt-/systemägare 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 Alingsås kommuns informationssäkerhetspolicy och dessa riktlinjer efterlevs och ska utse systemförvaltare IT för objekt/system.

Systemförvaltare IT

Systemförvaltare IT samverkar med motsvarande roller i verksamheterna och i det ansvaret ingår att IT-säkerhetsrelaterade mål och åtgärder i objekt/system nås samt genomförs.

Systemtekniker IT

IT-tekniker ansvarar för att utföra IT-säkerhetsrelaterade aktiviteter på uppdrag av objekt-/systemägare IT, systemförvaltare IT, och/eller IT-säkerhetsansvarig, eller IT-chef.

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, IT-chef är ansvarig.

Klassning av IT-resurser

IT-resurser ska klassas i enlighet med Alingsås kommuns modell för informationsklassning. Underliggande IT-resurser i form av infrastruktur, stödsystem m.m. ska ges *minst* motsvarande klassning. Underliggande IT-resurser kan 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.

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”.

Ägare till IT-resurser ansvarar för att säkerhetsnivån är tillräcklig över IT-resursens hela livscykel, såväl vid införande, under drift som under avveckling.

Användningsinstruktioner

Användare av IT-resurs ska få instruktion om kring hantering av IT-resurs, vilka villkor och vilket ansvar som gäller kring den åtkomst de fått sig tilldelad. Regler och/eller instruktioner ska baseras på IT-resursernas klassning och skyddskrav.

Regler och/eller instruktioner ska finnas oavsett om IT-resursen endast används inom IT-avdelningen, av medarbetare inom kommunen eller av externa användare.

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 Objekt-/systemägare IT
D.1.2	En komplett förteckning över samtliga IT-resurser ska upprättas och underhållas. 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, exempelvis ett system, på ett specificerat sätt. Behörigheter, eller åtkomsträttigheter, definierar vad en användare har rätt att utföra, t.ex. läsa, söka, skriva, radera, skapa eller köra ett program.

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

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

Det samlade systemet för styrning av åtkomst i en (eller flera) IT-resurs(-er) benämns behörighetskontrollsystem och utgörs vanligen av både tekniska system och administrativa rutiner. Detta system 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 mankan göra med den, t.ex. läsa, skriva, ändra, radera
- Loggning av användarens aktiviteter.

Identifiering och autentisering

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

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

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. Särskilda skäl för undantag kan finnas, exempelvis skyddade identiteter.
D.2.3	Vid åtkomst till information med **höga skyddskrav** avseende konfidentialitet eller riktighet ska stark autentisering användas.
D.2.4	Fjärråtkomst för inloggning med konton med höga behörigheter till IT-resurs med **höga skyddskrav** avseende konfidentialitet eller riktighet är inte tillåten.
D.2.6	Lösenord är alltid konfidentiell information som har **höga skyddskrav** och ska i alla skeden av sin livscykel skyddas mot åtkomst från alla andra än ägaren själv. För att minska risken för obehörig åtkomst ska följande skyddsfunktioner införas: • Tekniska funktioner implementeras där så är möjligt i IT-resursen för att säkerställa att lösenordsregler för medarbetare avseende historik, komplexitet och åldring av lösenord följs. • Lösenord ska aldrig skickas/transporteras i klartext över nätverk. I de fall detta inte är möjligt ska tillfälliga lösenord i kombination med tvingande lösenordsbyte användas. Tillfälliga lösenord ska enbart vara giltiga för en (1) inloggning. • Lösenord får aldrig lagras på ett sätt som gör det möjligt att dekryptera dem till klartext. Om felaktigt lösenord används mer än tre 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 skyddskrav** (se ovan).

För verksamhetssystem är det objektägare eller systemägare i verksamheten som beslutar vilka som ska få tillgång till systemet och vilka behörigheter dessa ska ha, samt hur systemet är klassat. Objekt-/systemägare IT ansvarar för att upprätta ett behörighetskontrollsystem som motsvarar dessa krav.

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

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

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 sekretessavtal.

För administrativa åtkomsträttigheter gäller att de ska vara restriktiva och ge endast de rättigheter som behövs för att utföra sitt uppdrag i den administrativa roll man har.

Regelbunden uppföljning och revision av samtliga åtkomsträttigheter ska ske kontinuerligt. För priviligierade användare med särskilda åtkomsträttigheter (administratörer) ska revision ske om möjligt med kortare intervall. Särskild uppmärksamhet kan behöva ägnas då medarbetare med priviligierade åtkomsträttigheter slutar eller byter tjänst. Processer och rutiner för behörighets- hantering ska följas upp och dokumenteras.

Riktlinjer för reglering av åtkomsträttigheter	
D.2.8	Det ska finnas beslutade och dokumenterade regler och rutiner för behörighetshantering för IT-resurser.
D.2.9	IT-resurser ska ha åtkomsträttigheter som motsvarar hur de är klassade.
D.2.10	Användaridentiteter och vilka individer dessa tillhör ska registreras i en gemensam 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 snarast. Det ska om möjligt finnas rutiner kopplade till personalavdelningen för att säkerställa att sådan reglering av åtkomst kan ske vid anställning, vid förändring av roll eller arbetsuppgifter samt vid upphörande av anställning.
D.2.13	Administrativa rättigheter ska endast ges där så är uttryckligen nödvändigt. För tilldelning av administrativa rättigheter för användare på klienter gäller att sådan rätt i första hand ska ges tillfälligt för att t.ex. omfatta en installation av programvara och i andra hand ges för en viss tid med ett specifikt slutdatum. IT objekt-/systemägare beslutar om tilldelning av priviligierad åtkomsträtt. Granskning av administrativa rättigheter ska ske i enlighet med verksamhetens behov och legala förutsättningar.
D.2.14	Gruppidentiteter är inte tillåtna. Eventuella undantag ska godkännas av Objekt-/systemägare verksamhet. Gruppidentiteter ska då enbart beviljas under följande förutsättningar: • Behov av gruppidentitet är tydligt beskrivet och alternativen utredda så att det framgår varför gruppidentiteten är nödvändig • Gruppidentiteten ska ha en registrerad ägare • Gruppidentiteten ska vara tidsbegränsade med tydligt slutdatum • En avvecklingsplan ska finnas för att ersätta gruppidentiteten med individuella identiteter • Ägaren av gruppidentiteten ska föra en förteckning alla som använder identiteten. Historikfunktion ska finnas så att förteckningen kan visa vilka användare somfanns viden given tidpunkt • Användande av gruppidentiteter ska dokumenteras enligt ovan.
	• 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 avgruppidentiteten • Ägaren av gruppidentiteten tar fullt ansvar för eventuellt missbruk avgruppidentiteten

.2.15	För externa användare gäller att tilldelning av åtkomst, utöver övriga regler för åtkomsttilldelning även ska: • Tidsbegränsas att endast omfatta tiden som behövs för att utföra uppgiften • Föregås av sekretessavtal

Säkerhetsloggning

För att möjliggöra incidentutredningar och att i efterhand kunna utreda vad som hänt krävs spårbarhet. För att erhålla spårbarhet ska kommunens IT- resurser övervakas och loggas avseende användaraktiviteter, avvikelser, fel och informationssäkerhetsincidenter. Loggar ska skyddas mot manipulation och obehörig åtkomst, sparas en viss tid och granskas regelbundet av utpekad loggadministratör.

I de fall logginformation går att knyta till en enskild person är de att betrakta som personuppgifter och omfattas då av krav i dataskyddsförordningen (GDPR).

Riktlinjer för säkerhetsloggning	
D.2.17	Vid åtkomst till IT-resurs och information med **höga skyddskrav** avseende konfidentialitet eller riktighet krävs loggning av åtkomst för att erhålla spårbarhet.
D.2.18	Loggningsverktyg och logginformation ska skyddas mot manipulation och obehörig åtkomst, logginformation innehållande loggning av åtkomst har alltid **höga skyddskrav** avseende konfidentialitet eller riktighet.
D.2.19	Händelseloggar som registrerar användaraktiviteter, avvikelser, fel och informationssäkerhetsincidenter, 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, såsom att genom kryptering förhindra obehörig åtkomst till information, eller genom kryptografiska signaturer garantera informationens riktighet eller äkthet.

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

Krypteringslösningar ska bygga på etablerade standarder och ska tas fram av objektägare IT i samråd med verksamhetsansvarig och IT-säkerhets- ansvarig. Införande av krypteringslösningar ska godkännas av informationssäkerhetsansvarig efter prövning av informationssäkerhetsrådet.

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

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

Riktlinjer för kryptering	
D.3.1	Krypteringslösningar ska baseras på etablerade standarder och införande ska godkännas av informationssäkerhetsrådet.
D.3.2	Nyckelhantering ska säkerställas för att tillgodose de krav som finns för IT-resurs avseende • Revokering av nycklar • Validering av nycklars giltighet och autenticitet • Återställning av nycklar
D.3.3	Krypteringsnycklar är **konfidentiell** information och ska skyddas därefter.

D4. Fysisk och miljörelaterad säkerhet

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

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 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. Instruktion för hur arbete i respektive lokal får bedrivas ska finnas. 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

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. Om underhåll och reparation ska utföras av extern personal på IT-resurs med **höga skyddskrav** avseende konfidentialitet ska extern personal alltid underteckna sekretessavtal. Det kan vara nödvändigt att vidta särskilda åtgärder, exempelvis att känslig information flyttas, raderas eller krypteras innan någon extern personal 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 behöva skrivas över eller destrueras innan den sänds till skrotning eller återanvändning.

Skydd av utrustning

Utrustning ska placeras och skyddas för att motverka stöld och miljörelaterade hot som värme, kyla, fuktighet, vätska samt partiklar i luft. Användning ska ske i enlighet med ägarens instruktioner. I publika lokaler krävs stöldskydd (t.ex. fastlåsning) och märkning av utrustning. Mobil utrustning som ska användas utanför kommunens lokaler ska förses med stöldskydd och märkning. Användning ska ske i enlighet med de instruktioner som gäller vid distansarbete och mobil utrustning.

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 försörjnings-system.

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 vatteninträngning hanteras. Om golvbrunn finns ska åtgärder vidtas för att undvika att vatten kan tränga upp.
D.4.9	Utrymmen som innehåller informationstillgångar med **höga skyddskrav** ska uppfylla Skyddsklass 3 enligt SSF 200 Inbrottsskydd.
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 extern personal ska utföra underhåll på IT-resurs med **höga skyddskrav** ska sekretessavtal 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 kommunarkivet, ske genom att information skrivs över, raderas eller förstöras.

D.4.16	Avveckling eller skrotning av datamedia med **höga skyddskrav** på konfidentialitet sker genom att information skrivs över i multipla operationer, alternativt att mediet där informationen lagrats förstörs på ett fullständigt och oåterkalleligt sätt. Observera att krypterad datamedia inte är känslig om nyckel för dekryptering ges ett fortsatt skydd, eller att nyckel destruerats.

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

Det ska finnas dokumenterade driftsrutiner tillgängliga för alla användare som behöver dem. Driftsrutiner ska vara formella och beslutade dokument, utgör del av systemdokumentation.

Driftsrutiner ska finnas för väsentliga processer och objekt, exempelvis:

- installation och konfiguration av system
- uppstarts- och nedtagningsrutin
- säkerhetskopiering,
- underhåll av utrustning
- supportkontakter vid oväntade funktionella eller tekniska problem
- hantering av media och datahall.

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

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

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.
D.5.3	Utvecklings-, test- och driftmiljöer ska vara separerade för att minska risken för obehörig åtkomst eller ändringar i driftmiljön.

Skydd mot skadlig kod

För att skydda mot skadlig kod behövs metoder för att förebygga, upptäcka skadlig kod och för att återställa IT-miljön efter angrepp.

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

Programvara ska i förebyggande syfte skanna efter skadlig kod i:

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

IT-resurser med **höga skyddskrav** ska regelbundet granskas med avseende på skadlig kod.

Om angrepp av skadlig kod inträffat ska det finnas en fastställd rutin för återställning av IT-resurser (se avsnitt D9 – Incidenthantering).

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 skydd mot skadlig kod som förebygger, upptäcker skadlig kod och som återställer i kommunens IT-miljö efter angrepp. Alla datorer (servrar och klienter) ska ha skydd mot skadlig kod (antivirusprogramvara) som frekvent och regelbundet uppdateras (dagligen)
D.5.5	IT-resurser som stöder objekt med **höga skyddskrav** ska regelbundet granskas med avseende på skadlig kod.
D.5.6	System och applikationer ska regelbundet uppdateras för att hållas fria från säkerhetsbrister som kan exploateras av skadlig kod. Säkerhetspatchar ska regelmässigt och skyndsamt installeras på alla IT- resurser enligt tillverkarnas rekommendationer och enligt fastställd rutin
D.5.7	Det ska finnas en fastställd rutin för återställning av datorer om kommunen skulle drabbas av skadlig kod eller virusutbrott.
D.5.8	Det ska finnas rutiner för att regelbundet samla in information om skadlig kod, t.ex. prenumerera på nyhetstjänster eller bevaka webbplatser som ger information om ny skadlig kod (t.ex. cert.se).

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 hos information.

Säkerhetskopieringen syftar till att väsentlig information ska kunna rekonstrueras med hjälp av säkerhetskopior och återlagringsrutiner.

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

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

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 om viktiga kvalitetsmått inte uppfylls. Gränsvärden för larm ska sättas så att uppfyllande av målsättning för återställningstid säkerställs. Automatiska larm ska regelbundet testas.
D.5.10	Baserat på objekts/systems klassning av riktighet och tillgänglighet ska krav definieras för säkerhetskopiering av information. Dessa krav ska minst reglera vilken information som ska omfattas av säkerhetskopiering, hur lång tid säkerhetskopior ska sparas samt vilka kontroller som ska genomföras av att säkerhetskopiorna fungerar. Vidare ska maximal informationsförlust och målsättning för återställningstid definieras för varje IT- resurs och tillsammans med övriga krav ligga till grund för vald backuplösning. • Målsättning för återställning av data, RPO (Recovery Point Objective), denmaximalt acceptabla mängden av dataförlust som tillåts vid en återställning av en IT-tjänst efter ett avbrott ska fastställas • Målsättning för återställningstid, RTO (Recovery Time Objective), den längsta acceptabla tiden för att återställa IT resursen efter ett avbrott ska fastställas
D.5.11	Det ska finnas en process för återlagring från säkerhetskopia som är testad och dokumenterad för respektive IT-resurs.
D.5.12	Backup av IT resurser med **höga skyddskrav** avseende tillgänglighet (höga RTO krav) bör lagras på snabbt backupmedia såsom t.ex. SAN-diskar. Övervakning av backupfunktion ska konfigureras med automatlarm vid problem.
D.5.13	Säkerhetskopiering av information med **höga skyddskrav** avseende konfidentialitet ska ske till krypterad backupmedia eller ges motsvarande skydd. Säkra återställningsrutiner ska användas med kontroller att återställning av konfidentiell information ges rätt skydd efter återställning, t.ex. bör dekryptering under återställning undvikas.
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 korttidlagrade 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 rapporter och varningar avseende säkerhet i system och tillämpningar.

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

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

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 objekt-/systemägares 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 skyddskrav** och ska skyddas mot manipulation och obehörig åtkomst.

Hantering av tekniska sårbarheter

Det ska finnas rutiner så att information om tekniska sårbarheter upptäcks i tid, att sårbarheter kan analyseras och att lämpliga åtgärder kan vidtas för att behandla de risker som sårbarheter medför.

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

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 säkerhetspatchningar ska göras regelbundet på IT-resurser.
D.5.21	I de fall säkerhetspatchning inte är praktiskt möjlig ska information om tekniska sårbarheter i sådana IT-resurser inhämtas och analyseras och lämpliga åtgärder vidtas för att hantera den tillhörande risken.
D.5.22	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 utförs av användare som definierar vilka typer av program en användare kan installera och på vilket sätt.

D6. Kommunikationssäkerhet

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

Nätverkssäkerhet

Det ska finnas rutiner för hantering av nätverk. Förvaltning ska ske av ansvariga som utpekas av ägare till nätverk.

Skyddsåtgärder ska införas för att nå säkerhet för information i nätverk och anslutna tjänster utifrån informationsklassningen av anslutna objekt. 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)

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

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 skyddskrav** avseende konfidentialitet är endast tillåtet från godkända klienter. Teknik för att kryptera och säkra kommunikationen ska alltid användas oavsett skyddskrav.
D.6.3	En grundläggande segmentering av nätverket ska göras för att skilja interna nät från Internet, samt att skilja utvecklings-, test- och produktionsmiljöer från varandra. Grupper av informationstjänster, användare och informationssystem kan ytterligare segmenteras i separata nätverks efter skyddsbehov. • Utrustning ska finnas för att kontrollera och förhindra obehörig nätverkstrafikmellan olika nätverkssegment.
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 brandväggspolicyer ska revideras periodiskt.
D.6.5	Kommunikationstjänster mellan Alingsås kommun och externa nätverk ska dokumenteras och godkännas av Objekt-/systemägare IT innan inkoppling får ske.

Informationsöverföring

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

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

Riktlinjer för informationsöverföring	
D.6.6	Kommunikation med **höga skyddskrav** avseende konfidentialitet och riktighet ska alltid krypteras och kommunicerande parter ska identifieras på ett säkert sätt med digitala signaturer eller motsvarande.
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 information mellan Alingsås kommun och externa parter ska regleras genom avtal där minst följande regleras: • Motparten informeras om informationens klassning och garanterar att information med normala eller **höga skyddskrav** avseende konfidentialitet ges rätt nivå av skydd och inte förs vidare till annan part. • Kommunikationslösning ska definieras med de nätverkskomponenter som ingår i säkerhetslösningen samt den konfiguration och de inställningar som krävs för att upprätthålla rätt nivå av skydd. • Vid kommunikation med annan part med normala eller **höga skyddskrav** avseende konfidentialitet ska överföringen skyddas med kryptering. • Trafik i uppsatta förbindelser ska om möjligt loggas av båda parter.
D.6.9	Kommunikation med e-post till andra organisationer skyddas i samtliga e-postsystem genom att konfigurera och aktivera standardiserade säkerhetsfunktioner.

D7. Anskaffning och utveckling av IT-resurser

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

Säkerhetskrav på IT-resurser

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

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

Utveckling, anskaffning eller förändring av system som omfattas av verksamhetsnära förvaltning ska involvera parterna i förvaltningsorganisationen. Objekt-/systemägare IT ansvarar för att rätt tekniska krav formuleras som överensstämmer med verksamhetens krav så att system ges skydd som korrelerar till klassningen. Utveckling, anskaffning eller förändring av underliggande IT-resurser i form av infrastruktur, stödsystem m.m. ska ha minst motsvarande krav som de system som de stöder. Ibland kan kraven vara ännu högre än för de system de stödjer, exempelvis om en IT-resurs stödjer ett stort antal system som var för sig inte är kritiska.

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

Riktlinjer för säkerhetskrav på IT-resurser	
D.7.1	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 standardsystem). Informationssäkerhetskraven ska baseras på den klassning som tilldelats IT-resursen och ska dokumenteras och granskas av alla berörda parter innan utvecklingen, anskaffningen eller förändringen påbörjas.

Säkerhetskrav vid upphandling av IT-stöd

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

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

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

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

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 enheten för upphandling.

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 både den operativa verksamheten och i arbetet med 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 innefatta: • Att leverantören innan leverans till Alingsås kommun genomför säkerhetstestning av system och ingående komponenter. Att leverantören ska åtgärda eventuella säkerhetsbrister som identifierats isamband med acceptanstest och/eller leveranskontroll.
D.7.6	Avtal med IT-leverantör ska reglera hur kontroll av avtalets uppfyllande ska ske, t.ex. genom tredjepartsrevision eller granskning genomförd av Alingsås Kommun.
D.7.7	Upphandling av system som ska driftas hos extern leverantör medför ytterligare krav, exempelvis: • Fördjupade krav på leverantörens interna IT-miljö ochinformationssäkerhet (t.ex. certifieringar) • Leverantörens kontinuitetshantering • Rätt till tredjepartsrevision • Sekretessavtal • Personuppgiftsbiträdesavtal • Rätt till incidentrapporter från leverantören som berör Alingsås kommun
D.7.8	Upphandling av IT-stöd ska göras i samverkan med upphandlingsenheten.
D.7.9	Om IT-leverantör använder underleverantör för hela eller del av leveransen ska ett avtal tecknas dem emellan som reglerar såväl affärsmässighet som säkerhet. Avtalet ska kunna delges. Följande punkter ska då minst beaktas avseende säkerhet: • Hur applicerbara krav i avtal med IT-leverantör säkerställs även mot dessunderleverantör • Hur rättsliga krav uppfylls, exempelvis rörande lagstiftning om sekretess och personuppgifter • Vilka åtgärder som vidtas för att säkerställa att alla berörda parter, inklusive underleverantörer, är medvetna om sitt säkerhetsansvar, licensieringsarrangemang, äganderätt till koden och upphovsrätt • Vilka åtgärder som vidtas för att säkerställa kvalitet i leverans från underleverantör

Säkerhet vid systemutveckling

Regler för säker utveckling av program och system ska upprättas och tillämpas vid systemutveckling.

Systemförändringar inom utvecklingscykeln ska styras genom användning av ändringshanteringsprocessen.

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

Outsourcad systemutveckling ska övervakas och styras efter behov.

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 ändringshanteringsprocessen.
D.7.13	För systemutvecklings- och integrationsåtgärder ska utvecklingsmiljöer upprättas och skyddas över IT- resursens hela livscykel.
D.7.14	Systemutvecklare ska ha kompetens i programvarusäkerhet.
D.7.15	Outsourcad systemutveckling ska övervakas och styras efter behov.

Säkerhetskrav vid test

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

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

Test-, utvecklings- och driftmiljöer ska om möjligt separeras för att minska risken för obehörig åtkomst eller ändringar i produktionsmiljön.

Driftsättning ska ske enligt ändringshanteringsprocessen.

Riktlinjer för säkerhetskrav vid test	
D.7.16	Säkerhetsfunktionalitet ska testas vid utveckling och testning ska göras gentemot de ställda säkerhetskraven och i enlighet med överenskommen säker utveckling.
D.7.17	Produktionsdata ska inte användas i test utan all testdata ska väljas ut noggrant, skyddas och styras. Om produktionsdata ändå behöver används gäller följande: • 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 objekt-/systemägare IT varje gång produktionsdata kopieras till etttestsystem • 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 om möjligt separeras för att minska risken för obehörig åtkomst eller ändringar i produktionsmiljön.
D.7.19	Driftsättning ska ske enligt ändringshanteringsprocessen.

D8. Incidenthantering

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

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.

Viktiga aktiviteter i incidenthanteringsprocessen är

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

Incidenter drivs av objekt-/systemägare, IT-avdelning och övriga berörda parter är delaktiga i lösning av problemet.

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.

Större incidenter ska sammanställas i incidentrapporter som respektive objekt-/systemägare ansvarar för att ta fram i samverkan med IT-avdelningen. Mindre incidenter bör 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 incidenthanteringsprocess som omfattar informationssäkerhetsincidenter. Processen ska innefatta: • Mottagning av information om incidenten • Styrning av eventuella behov av omedelbara åtgärder. Dessa kan vara av temporärart tills en mer hållbar lösning kan komma på plats • Analys av orsaker till incidenten så åtgärder kan vidtas • Återkoppling och kommunikation med dem som är påverkade aveller involverade i återställandet till normal drift.
D.8.2	Större incidenter ska sammanställas i incidentrapporter som respektive objekt-/systemägare ansvarar för att ta fram i samverkan med IT-avdelningen.
D.8.3	Erfarenheter från inträffade incidenter, t.ex. genom incidentrapporter och statistik, ska ligga till grund för framtida beslut för att förbättra skyddet, t.ex. att investera i nya säkerhetslösningar.
D.8.4	Medarbetare är skyldiga att rapportera informationssäkerhetsincidenter såväl som informations- och IT-relaterade brister i system eller tjänster.
D.8.5	Incidenter där brott eller misstanke om brott föreligger ska alltid polisanmälas.

Krisorganisation och krisplan

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

D9. 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 verksamhets-processer och dessas beroenden av stöd och resurser som t.ex. personal, lokaler och verktyg.

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

Detta innebär att det för objekt/system med **höga skyddskrav** avseende tillgänglighet måste finnas en beredskap för hur man hanterar avbrott . Objekt-/systemägare ansvarar för att kontinuitetsplan finns på plats och att de motsvarar de krav som finns för objekt/system.

Målsättningen är att kontinuitetshantering ska utvecklas i hela Alingsås kommun och på sikt ingå i ett ledningssystem för informationssäkerhet.

Riktlinjer för kontinuitetshantering	
D.9.1	Det ska finnas kontinuitetsplaner för samtliga kritiska IT-resurser med **höga skyddskrav** avseende tillgänglighet.
D.9.2	Övning och testning av kontinuitetsplaner ska genomföras och utvärderas regelbundet och identifierade brister samt svagheter åtgärdas med syfte att ständigt förbättra kontinuiteten för IT.
D.9.3	Kontinuitetsplaner ska finnas tillgängliga för de medarbetare som ingår i aktiviteterna, men samtidigt utgör planerna information med **högt skyddsvärde** och förvaras skyddat så att de inte blir åtkomliga för obehöriga.

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. Särskilt viktigt är det att genomföra kontroll och granskning av kritiska delar av IT-miljön som direkt eller indirekt stöder system med **höga skyddsvärden**, samt införande av nya IT-lösningar.

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

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

Riktlinjer för granskning och kontroll	
D.10.1	Kritiska delar i IT-miljön som stödjer objekt med **höga skyddsvärden** 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.
D.10.3	Sårbarheter och brister som upptäcks vid granskningar ska tas upp för åtgärdande i genomförandeplaner. 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 delar av IT-miljön ska göras minst vartannat år. Innan granskning eller revision kan ske ska följande beaktas: • Behov på åtkomst till system och data inför granskning eller revision ska avtalas med objekt-/systemägare • Omfattningen av tekniska aktiviteter för granskning eller revision ska beskrivas för- och godkännas av IT-resursens ägare. • Aktiviteter vid granskning eller revision begränsas om möjligt tillskrivskyddad åtkomst av program och data • Granskning som kan påverka tillgänglighet bör utföras vid sådan tidpunkt då påverkan på verksamheten är så liten som möjligt • All åtkomst vid granskning eller revision ska övervakas och loggas