

Riktlinjer för informationssäkerhet



Dokumenttyp	Riktlinje
Dokumentnamn	Riktlinje för informationssäkerhet
Antagen av:	Kommunfullmäktige
Diarienummer	
Giltighetstid	Tills vidare
Gäller för	Avesta kommunkoncern
Sammanfattning	
Granskad	
Reviderad	
Dokumentansvarig	Kommunstyrelsen
Webbansvarig	Webbredaktör kommunstyrelsen
Publiceras	Extern webb
Relaterade dokument	Policy för informationssäkerhet

Innehåll

1. Inledning.....	5
1.1 Riktlinjernas omfattning.....	5
1.2 Struktur och läsanvisningar.....	5
1.3 Introduktion till informationssäkerhet.....	6
1.4 Termer och definitioner	7
Kapitel A: Styrning av informationssäkerhet	8
2. Inledning.....	9
2.1 Roller, ansvar och organisation	9
3. Dokumentstruktur	11
3.1 Informationsklassning	12
4. Ledningssystem för informationssäkerhet	13
4.1 Personalsäkerhet.....	14
5. Efterlevnad och granskning.....	15
Kapitel B: Informationssäkerhet för medarbetare	16
6. Inledning.....	17
7. Medarbetares ansvar för informationssäkerhet	17
7.1 Skyldighet att rapportera incidenter och brister	17
7.2 Säkert beteende.....	17
7.3 Lösenord.....	18
7.4 Enheter.....	19
7.5 E-post.....	22
7.6 Lagring och säkerhetskopiering	22
7.7 Spårbarhet och loggning.....	23
8. Informationsklasser	23
8.1 Personuppgifter	24
8.2 Allmänna handlingar och sekretess	24
Kapitel C - Informationssäkerhet i verksamhetsnära förvaltning.....	25
9. Inledning.....	26
10. Roller och ansvar.....	26
11. Dokumentation av informationssäkerhet	26
12. Informationsklassning och systemklassning.....	27
13. Behörighetshantering och loggning	27
13.1 Behörighetstilldelning.....	27
13.2 Ansvar för behörighetstilldelning	27
13.3 Rutiner för behörighetsförvaltning och revision.....	27
13.4 Logghantering	28
14. Ändringshantering	28

15. Användarinstruktioner	28
16. Risk- och sårbarhetsanalyser	29
17. Incidenthantering	29
18. Kontinuitetshantering	30
Kapitel D – Informationssäkerhet i IT-miljön	31
19. Inledning.....	32
20. Roller och ansvar.....	32
20.1 Roller i den IT-nära förvaltningen.....	32
21. Hantering av tillgångar	33
21.1 Identifiering av IT-resurser och tilldelning av ägare.....	33
21.2 Klassning av IT-resurser	33
21.3 Instruktioner för användare.....	33
22. Styrning av åtkomst	34
22.1 Identifiering och autentisering	34
22.2 Reglering av åtkomsträttigheter	35
22.3 Säkerhetsloggning.....	36
22.4 Kryptering	37
23. Fysisk och miljörelaterad säkerhet.....	38
23.1 Säkra utrymmen för IT-resurser	38
23.2 Godsmottagning och lastning.....	38
23.3 Underhåll, reparation och avveckling	38
23.4 Skydd av utrustning.....	38
23.5 Elförsörjning.....	39
24. Driftsäkerhet.....	40
24.1 Driftsrutiner	40
24.2 Skydd mot skadlig kod	40
24.3 Säkerhetskopiering	41
24.4 Loggning och övervakning	42
24.5 Hantering av tekniska sårbarheter	43
25. Kommunikationssäkerhet.....	43
25.1 Nätverkssäkerhet.....	43
25.2 Informationsöverföring.....	44
26. Anskaffning och utveckling av IT-resurser	45
26.1 Säkerhetskrav på IT-resurser.....	45
26.2 Säkerhetskrav vid upphandling av IT-stöd	45
26.3 Säkerhet vid systemutveckling.....	46
26.4 Säkerhetskrav vid test	47
27. Incidenthantering.....	48
28. Krisorganisation och krisplan	48

28.1 Kontinuitetshantering.....	49
29. Granskning och kontroll.....	49

1. Inledning

Avesta kommuns policy för informationssäkerhet är ett dokument som redovisar kommunens övergripande mål och inriktning med informationssäkerhet. Detta dokument – Riktlinjer för informationssäkerhet konkretiserar policyn för informationssäkerhet med mer detaljerad information och regler för hur information får hanteras inom kommunen. Vidare finns det regler som beslutas av exempelvis IT- och digitaliseringschef som mer i detalj styr vissa delar av informationssäkerheten.

1.1 Riktlinjernas omfattning

Riktlinjerna innehåller information och regler gällande säkerhet vid all hantering av information inom Avesta kommun.

Riktlinjerna gäller för alla verksamheter i Avesta kommun, inklusive bolag, vilket medför att det normalt inte finns utrymme att besluta om lokala regler som avviker från dessa.

1.2 Struktur och läsanvisningar

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

Kapitel	Innehåll	Primär målgrupp	Sidor
A	Styrning av informationssäkerhet	Alla som arbetar med IT- och informationssäkerhet	8–15
B	Informationssäkerhet för medarbetare	Alla medarbetare	16–24
C	Informationssäkerhet i verksamhetsnära förvaltning	Informations- och systemägare samt förvaltningsledare	25–30
D	Informationssäkerhet i IT-miljön	Chef och medarbetare på IT-och digitaliseringsenheten	31–50

Varje kapitel består både av informativa avsnitt och av riktlinjer som är obligatoriska. Samtliga riktlinjer är numrerade och i tabellform.

Kapitel B – Informationssäkerhet för medarbetare – har strukturerats för att stämma överens med avsnitten i utbildningen DISA (Datorstödd informationssäkerhetsutbildning för användare). DISA har skapats av MSB - Myndigheten för samhällsskydd och beredskap - och utgörs av ett antal filmer med tillhörande information. Tanken är man ska kunna genomgå DISA-utbildningen parallellt som man läser riktlinjerna i Kapitel B - Informationssäkerhet för medarbetare.

Informationsklassning är en central del i kommunens arbete med informationssäkerhet och finns med genomgående i riktlinjerna. Hur information klassas ska styra i vilken grad informationen ska skyddas. Modell för informationsklassning beskrivs i Kapitel A och information och regler för hur information ska klassas och skyddas utifrån denna återfinns i respektive kapitel.

1.3 Introduktion till informationssäkerhet

Informationssäkerhet handlar om att se till att informationstillgångar finns tillgängliga när de behövs, att de är korrekta och att obehöriga inte får åtkomst till dem. En väl utvecklad och integrerad informationssäkerhet bidrar till att etablera en effektiv och ändamålsenlig informationshantering, vilket skapar förtroende både inom och utanför organisationen och direkt bidrar till att:

- undvika incidenter,
- verksamhetsutveckling sker med rätt säkerhet,
- bevara förtroendet hos medborgarna, samt
- införa en metodik och ett arbetssätt för att efterleva lagstiftning och löpande uppföljning.

Informationssäkerhet är orienterat mot verksamhet, eftersom det handlar om säkerhet för information som har ett värde och en betydelse i en verksamhet. Informationens relevans och värde är avgörande vid bedömning av vilken grad av skydd som är rimlig i en viss situation. Det är informationens värde som styr vilken säkerhet som krävs, i form av till exempel fysiskt skydd som lås, passersystem och brandskydd eller vilken IT-säkerhet som krävs. Informationssäkerhet handlar om bevarande av konfidentialitet, riktighet och tillgänglighet (KRT).

Begrepp	Innebörd
Konfidentialitet	Att information enbart är tillgänglig för behöriga.
Riktighet	Att information är korrekt, tillförlitlig och fullständig.
Tillgänglighet	Att information är åtkomlig i rätt tid och användbar av behörig.

Informationssäkerhet begränsas inte till säkerhet i IT-resurser utan det omfattar information i alla dess former och oavsett hur informationen hanteras. De tre aspekterna KRT gällande en viss informationsmängd kan ha både interna krav eller härledas från rättsliga krav eller förväntningar och behov från externa aktörer. Rättsliga krav omfattar bland annat lagar, förordningar, föreskrifter och avtal. Externa aktörer har ofta behov och förväntningar som påverkar organisationens informationssäkerhet, exempelvis hur enkel viss information ska vara att ta del av för allmänheten. Vad som är lämplig nivå av skydd för en viss informationsmängd beror på dessa krav, hotbild, och i vilka situationer informationen hanteras – hur den lagras, bearbetas, kommuniceras och så vidare.

Olika typer av händelser (incidenter), som kan vara avsiktliga eller oavsiktliga, kan försämra konfidentialiteten, riktigheten eller tillgängligheten hos informationstillgångar. Information kan till exempel stjälas, raderas, förändras på ett oönskat sätt eller göras otillgänglig.

1.4 Termer och definitioner

I tabellen definieras några av de centrala begreppen inom informationssäkerhet. Roller beskrivs under rubrikerna 2 och 20.

Term	Definition
Autentisering	Verifiering av att en användare eller IT-resurs är den som den utger sig för att vara.
Behörighet	Tilldelade rättigheter att använda information eller en IT-resurs på ett specificerat sätt.
Data	Information i form av till exempel tecken eller signaler som är lämpad för överföring, tolkning eller bearbetning av människor eller av automatiska hjälpmedel.
Information	Innebörd i data, det vill säga data tolkad av människor.
Informationsklassning	Att genom konsekvensanalys identifiera skyddsbehovet för en viss informationsmängd.
Informationssäkerhet	Konfidentialitet, riktighet och tillgänglighet hos information.
Informationssäkerhetspolicy	Kommunens viljeinriktning med informationssäkerhet.
Informationstillgång	Information som är av värde för organisationen, och även de resurser som hanterar den, exempelvis människor, papper, mjukvara, hårdvara och immateriella tillgångar (till exempel rykte).
IT-resurs	IT-baserad komponent som hanterar information, till exempel 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 enbart är tillgänglig för behöriga.
Ledningssystem för informationssäkerhet (LIS)	Ett administrativt ramverk som syftar till att upprätta, införa, driva, övervaka, granska, underhålla och förbättra organisationens arbete med informationssäkerhet.
Riktighet	Att information är korrekt, tillförlitlig och fullständig.
Sekretess	Information som inte får lämnas ut och bli allmänt tillgänglig. Sekretessbelagd uppgift innebär tystnadsplikt för den som har tagit del av uppgiften.
Spårbarhet	Utförda aktiviteter som kan spåras till en identifierad användare eller IT-resurs.
Tillgänglighet	Att information är åtkomlig i rätt tid och användbar av behörig.

Kapitel A: Styrning av informationssäkerhet

2. Inledning

Detta kapitel beskriver och reglerar hur arbetet med informationssäkerhet ska bedrivas i Avesta kommun. Den primära målgruppen för detta kapitel är de som arbetar med informations- och IT-säkerhet eller har ansvar för informationssäkerhet i förvaltningsobjekt, projekt, processer eller andra verksamheter.

I kapitlet ges en introduktion till informationsklassning och den modell för informationsklassning som Avesta kommun antagit i och med dessa riktlinjer.

2.1 Roller, ansvar och organisation

2.1.1 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 och så vidare) också är ansvarig för informationssäkerheten inom verksamhetsområdet.

Kommunens informationssäkerhetsansvarige och övriga som arbetar specifikt med informationssäkerhet, IT-säkerhet eller andra relaterade frågor fungerar som stöd till medarbetare, verksamheter och kommunledningens möjlighet att kunna ta ansvar för informationssäkerheten.

2.1.2 Övergripande ansvar

Instans	Ansvar
Kommunfullmäktige	Fastställer övergripande principer för informationssäkerhetsarbetet genom en kommunövergripande informationssäkerhetspolicy.
Kommunstyrelsen/bolagsstyrelse	Ansvarar för att kommunens informationssäkerhetspolicy följs och för samordning av informationssäkerhetsarbetet i kommunen. Kommunstyrelsen ansvarar också för utarbetning och fastställande av riktlinjer för informationssäkerhet.
Kommundirektören/VD	Har ansvar för att informationssäkerhetsarbetet bedrivs i linje med den av fullmäktige fastställda informationssäkerhetspolicyen.
Ledningen	Ansvarar för att alla medarbetare i Avesta kommun efterlever informationssäkerhetspolicyen och riktlinjer för informationssäkerhet. Visar sitt stöd för dessa dokument och fungerar som förebild.

2.1.3 Ansvar inom respektive verksamhet

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

Verksamhetsansvarig, oavsett nivå, ansvarar för informationssäkerheten inom sin verksamhet. Varje verksamhetsansvarig ska se till att dennes medarbetare efterlever riktlinjer, har ett säkerhetsmedvetande

samt tillräcklig förståelse och kunskap för att en nödvändig informationssäkerhet i verksamheten ska uppnås.

Säkerhetsansvaret i sig kan inte delegeras, däremot kan ansvaret att genomföra vissa arbetsuppgifter fördelas.

2.1.4 Medarbetares ansvar

Alla medarbetare har ett ansvar för verksamhetens informationssäkerhet. Varje anställd ska i sitt arbete följa riktlinjer för informationssäkerhet samt eventuella verksamhets-specifika regler. Varje anställd är även skyldig att rapportera informationssäkerhetsrelaterade brister och incidenter.

2.1.5 Personuppgiftsansvar

Kommunstyrelsen och övriga nämnder/bolag är personuppgiftsansvariga inom respektive verksamhetsområde och ska utse dataskyddsombud som i sin tur ska ha hjälp av utsedda personuppgiftshandläggare inom verksamheterna. Som personuppgiftsansvariga har nämnderna det yttersta ansvaret för all behandling av personuppgifter inom sitt verksamhetsområde även om den personuppgiftsansvarige har utsett ett dataskyddsombud.

2.1.6 Kommunarkivet

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

2.1.7 Systemägares ansvar

Systemägare ansvarar för att förvaltningsobjekt efterlever informationssäkerhetspolicy och riktlinje för informationssäkerhet. En viktig del i ansvaret är att besluta om objektets informationssäkerhetsnivåer genom att klassning sker i enlighet med Avesta kommuns modell för informationsklassning. I den mån det inte finns utpekade systemägare följer ansvaret verksamhetsansvaret. Informationssäkerhetsansvar hos övriga roller inom förvaltningsorganisationen beskrivs i kapitel C.

2.1.8 Ansvar i projekt

Utsedd projektägare säkerställer att säkerhetsfrågorna beaktas. Styrgruppen är ansvarig för att säkerhetsfrågorna beaktas och ska tillsammans med projektägaren fastställa säkerhetsnivån för det som utvecklas. Projektledaren tillsammans med styrgrupp ansvarar för att fastslagen säkerhetsnivå beaktas i projektarbetet.

2.1.9 IT-enhetens ansvar

IT-enheten ansvarar för att säkerheten i kommunens IT-miljö som tjänster, processer, system, infrastruktur, verktyg etcetera är tillräcklig och uppfyller verksamhetens krav, legala krav samt informationssäkerhetspolicyn och riktlinjerna för informationssäkerhet.

2.1.10 IT-säkerhetsansvarig

Det ska finnas en utpekad IT-säkerhetsansvarig som samordnar arbetet med säkerheten i kommunens IT-miljö och som är stödjande vid kravställning på externa aktörer. Rollen IT-säkerhetsansvarig beskrivs utförligare i Kapitel D.

2.1.11 Informationssäkerhetsansvarig

Informationssäkerhetsarbetet i kommunen leds och samordnas av en informationssäkerhetsansvarig. Informationssäkerhetsansvarig ansvarar för:

- lyfta strategiska frågor till ledningen
- planera och samordna organisationens övergripande informationssäkerhetsarbete
- utveckla arbetssätt och processer
- förvalta kommunens styrande dokument inom området
- stötta verksamheten i genomförandet genom till exempel rådgivning
- utvärdera och följa upp resultat
- omvärldsbevakning inom informationssäkerhetsområdet,
- att rapportera läge och status gällande informationssäkerhet till kommunstyrelsen en gång per år, oftare om särskilda skäl finns som allvarigare incidenter, brister eller behov
- leda kommunens informationssäkerhetsråd.

2.1.12 Informationssäkerhetsrådet

Informationssäkerhetsrådet leds av informationssäkerhetsansvarig, som utser övriga ledamöter, inklusive kommunens och bolagens säkerhetschefer. Informationssäkerhetsrådet ska sammanträda 2–3 gånger per år och har till uppgift och befogenheter att:

- gå igenom inkomna incidenter och dra lärdomar/följa upp
- bereda dokument, till exempel styrande dokument, metoder och vägledningar,
- vara ett forum för erfarenhetsutbyte och omvärldsbevakning.

3. Dokumentstruktur

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

- Informationssäkerhetspolicy
- Riktlinje för informationssäkerhet
- Informationssäkerhetsanalys
- Handlingsplan för informationssäkerhet

Informationssäkerhetspolicy och riktlinje för informationssäkerhet riktar sig till alla medarbetare inom Avesta kommun medan informationssäkerhetsanalys och handlingsplan för informationssäkerhet riktar sig främst till de som arbetar med styrning av informationssäkerhet.

Styrdokument	Definition
Informationssäkerhetspolicy	Ett övergripande dokument som uttrycker ledningens viljeinriktning med informationssäkerhet. Beslutas av kommunfullmäktige och uppdateras vid behov.
Riktlinje för informationssäkerhet	Innehåller regler för hantering av information. Riktlinjen är uppdelade i kapitel för olika målgrupper. Beslutas av kommunfullmäktige och uppdateras vid behov.
Informationssäkerhetsanalys	En genomlysning av informationssäkerheten i kommunen innefattande hotbild, skyddsnivåer, kommunens inriktning samt interna och externa krav. Analysen genomförs i full skala vart

	fjärde år, men justeringar kan göras löpande beroende på förändringar i kommunen eller omvärlden. Informationssäkerhetsanalysen ligger till grund för hur arbetet med informationssäkerhet ska bedrivas och innehåll och utformning av de övriga dokumenten.
Handlingsplan för informationssäkerhet	Tas fram årligen och innehåller konkreta mål och åtgärder baserade på informationssäkerhetsanalysen.

Metoder, vägledningar och andra stöddokument kan tas fram centralt för att stödja arbetet med informationssäkerhet på olika nivåer och att underlätta tillämpningen och efterlevnaden av informationssäkerhetspolicy och riktlinjen för informationssäkerhet. Lokalt, till exempel i förvaltningar och på IT-enheten, kan mer specifika instruktioner och vägledningar tas fram i syfte att komplettera eller förtydliga riktlinjerna för informationssäkerhet.

Riktlinjer för dokumentstruktur för informationssäkerhet	
1.	Avesta kommuns informationssäkerhet och dess behov ska analyseras i en informationssäkerhetsanalys. Analysen ska genomföras minst vart fjärde år och ska ligga till grund för hur arbetet med informationssäkerhet ska bedrivas och innehåll och utformning av övriga styrande dokument.
2.	Årliga handlingsplaner för informationssäkerhet ska tas fram baserade på informationssäkerhetsanalyser.
3.	Det ska finnas en övergripande informationssäkerhetspolicy som uttrycker ledningens viljeinriktning med informationssäkerhet.
4.	Det ska finnas kommunövergripande riktlinjer för informationssäkerhet som konkretiserar informationssäkerhetsstrategin och som riktar sig till relevanta målgrupper.
5.	Det ska finnas modeller, metoder, vägledningar och andra stöddokument som stödjer olika gruppers efterlevnad av informationssäkerhetsstrategin och riktlinjerna för informationssäkerhet.

3.1 Informationsklassning

Informationsklassning är en grundläggande komponent i informationssäkerhetsarbetet. Genom att klassa information utifrån interna och externa krav på dess konfidentialitet, riktighet och tillgänglighet skapar man förståelse för och kan styra vilket skydd som krävs för olika informationsmängder. Främst handlar det om att skyddet ska bli tillräckligt, men ibland också för att undvika överskydd – med onödigt höga kostnader eller merarbete som följd. Klassning av information ska ske utifrån rättsliga krav som lagar och föreskrifter, men även interna krav på informationens värde, känslighet och betydelse för Avesta kommuns verksamheter.

I den vägledande standarden ISO 27002 rekommenderas att man ska ta fram en organisationsgemensam modell för informationsklassning. I Avesta 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 med mera. Denna typ av information kräver mer långtgående säkerhetsåtgärder

Riktlinjer för informationsklassning	
1.	Avesta kommun ska ha en gemensam modell för informationsklassning.
2.	Avesta 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.

3.1.1 Vad ska klassificeras?

Det är informationen som är den primära tillgången och som ska klassas och som sedan styr vilka skyddsåtgärder de olika nivåerna av skydds krav medför. Resurser som används för att hantera informationen, till exempel programvaror, tjänster och fysiska tillgångar, ska utformas och anpassas till de krav som klassningen i förlängningen ställer på dessa.

IT-system ska klassas på grundval hur informationen är klassad som finns i eller hanteras av systemen. En viktig uppgift för system- och informationsägare är därför att klassa sina system så att rätt skydds krav ställs. Riktlinjer för detta finns i kapitel C.

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

3.1.2 Användningsområden och målgrupper

Klassningsmodellen vänder sig till de i kommunen som är verksamhetsansvariga och/eller ägare av information och förvaltningsobjekt. Den vänder sig även till de som ansvarar för att rätt nivå av skydd skapas och upprätthålls. Den klassade informationen utgör ett underlag för en verksamhet vid kravställning av tjänster, exempelvis IT-tjänster, både internt och externt. Resultatet av klassningsarbetet kan därigenom fungera som ett gemensamt ramverk vid förhandling mellan beställare och leverantör av tjänster.

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

För de flesta medarbetare gäller endast aspekten Konfidentialitet, vilket betonas i kapitel B.

4. Ledningssystem för informationssäkerhet

I Avesta kommuns informationssäkerhetspolicy anges att kommunen ska bedriva ett systematiskt informationssäkerhetsarbete som baseras på standardserien ISO 27000 med målet att skapa ett ledningssystem för informationssäkerhet (LIS).

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

Ett systematiskt arbete med informationssäkerhet enligt ett LIS syftar till att informationssäkerheten över tid anpassas efter interna och externa förutsättningar och som därigenom upprätthåller en lämplig skyddsnivå över tid.

4.1 Personalsäkerhet

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

4.1.1 Före och i samband med anställning

Bakgrundskontroll av sökande till tjänster i kommunen ska ske genom verifiering av sökandes meritförteckning, till exempel genom kontakt med referenser och bekräftelse av påstådda akademiska och yrkesmässiga kvalifikationer. Lagstiftningen om registerkontroll för skydd av barn och unga ska efterlevas. För vissa kritiska tjänster krävs en förstärkt kontroll i form av exempelvis kreditupplysning och kontroll i brottsregister. Sådana 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 således 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 kommunens säkerhetsskyddsplan. Säkerhetsprövningen administreras av enheten kommunskydd vid kommunkansliet för förvaltningarna medan bolagens säkerhetsskyddschefer administrerar den för bolagen.

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

Nyanställda ska informeras ansvar och skyldigheter kopplade till informationssäkerhet och genomgå utbildning i informationssäkerhet. Information och utbildning ska också ges kopplat till annat ansvar som följer med rollen, till exempel informationsägarskap. Alla anställda som får tillgång till konfidentiell information ska underteckna ett sekretessavtal som även ska gälla efter avslut av anställning.

Riktlinjer för personalsäkerhet före och i samband med anställning	
1.	Bakgrundskontroll av sökande ska göras före anställning där sökandes meritförteckning verifieras.
2.	Anställning av kritiska roller ska genomgå förstärkt kontroll i form av kreditupplysning och kontroll i brottsregister.
3.	För befattningar som har betydelse för rikets säkerhet, är placerade i skyddsklass och som omfattas av Säkerhetsskyddslagen (2018:585) ska det i anställningsförfarandet genomföras en registerkontroll.
4.	Nyanställda ska informeras om ansvar och skyldigheter kopplade till informationssäkerhet och genomgå utbildning i ämnet. Nyanställda ska vidare ta del av kapitlet Informationssäkerhet för medarbetare i dessa riktlinjer samt informeras om annat ansvar som följer med rollen, till exempel informationsägarskap.
5.	Anställda som får tillgång till konfidentiell information ska underteckna ett sekretessavtal.

4.1.2 Under anställning

Alla medarbetare och i förekommande fall externa aktörer ska få utbildning för att kunna efterleva kommunens informationssäkerhetspolicy och riktlinje för informationssäkerhet. I enlighet med informationssäkerhetspolicyn ska medarbetare inom kommunen ha ett högt medvetande avseende informationssäkerhet. Roller som har särskilda uppgifter inom informationssäkerhet, till exempel inom IT-säkerhet eller systemförvaltningsorganisationen ska få lämplig fortbildning inom området som är relevant

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

Riktlinjer för personalsäkerhet under anställning	
1.	Alla medarbetare och i förekommande fall externa aktörer ska erhålla lämplig utbildning för att kunna efterleva kommunens informationssäkerhetsstrategi och riktlinjer för informationssäkerhet.
2.	Roller som har särskilda uppgifter inom informationssäkerhet ska få lämplig fortbildning inom området som är relevant för deras befattning.
3.	Det ska finnas en formell och kommunicerad disciplinär process för att vidta åtgärder mot anställda som har brutit mot gällande informationssäkerhetsregler.

4.1.3 Avslut eller ändring av anställning

Vid avslut eller ändring av anställning kan ansvar och skyldigheter för informationssäkerhet fortsätta att gälla, exempelvis sekretessavtal och tystnadsplikt om den anställde haft tillgång till konfidentiell information. Chef ansvarar för att detta kommuniceras till den anställde vid anställning/tillträddande av roll. Åtkomsträttigheter till information ska upphöra, och återlämning av IT-resurser ska ske, i direkt samband med avslut eller ändring av anställning.

Riktlinjer för avslut eller ändring av anställning	
1.	Ansvar och skyldigheter för informationssäkerhet som förblir gällande efter avslut eller ändring av anställning ska definieras och kommuniceras vid anställningstillfället eller tillträddande av roll och framgå i sekretessavtal.
2.	Återlämnande av IT-resurser och indrag av åtkomsträttigheter till information och IT-resurser ska ske i direkt samband med avslut eller ändring av anställning.

5. Efterlevnad och granskning

Efterlevnad av de styrande dokumenten Informationssäkerhetspolicy och Riktlinje för informationssäkerhet ska följas upp årligen inom ramen för internkontrollen. Det gäller särskilt de säkerhetsåtgärder som gäller för information, objekt och IT-resurser med höga skydds krav.

Revision av hela eller stora delar av kommunens informationssäkerhet ska göras minst vartannat år. Granskning av efterlevnad av informationssäkerhet kan genomföras av extern part, exempelvis på uppdrag av kommunrevisionen.

Sårbarheter och brister som upptäcks vid granskningar ska tas upp för åtgärdande i handlingsplaner. Akuta sårbarheter och brister ska åtgärdas omedelbart.

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 kapitlet Informationssäkerhet i IT-miljön.

Kapitel B: Informationssäkerhet för medarbetare

6. Inledning

Detta kapitel vänder sig till alla medarbetare i Avesta kommun. Riktlinjerna gäller även extern personal som har åtkomst till Avesta kommuns information, exempelvis inhyrda konsulter. Riktlinjerna beskriver det ansvar du som medarbetare har vid hantering av information i Avesta kommun och vilka regler som gäller. Avesta kommun är en stor organisation med många skilda verksamheter. Kompletterande regler till riktlinjerna kan därför finnas lokalt. Kontakta ansvarig chef om du är osäker på vad som gäller. Informationssäkerhet för medarbetare följer i stort en struktur framtagen av Myndigheten för samhällsskydd och beredskap – MSB – som finns i en utbildning för informationssäkerhet: DISA (Datorstödd Informationssäkerhetsutbildning för användare). Tanken är att man kan genomgå DISA-utbildningen och parallellt se vilka riktlinjer som gäller i Avesta kommun.

7. Medarbetares ansvar för informationssäkerhet

Information är en viktig resurs för Avesta kommun som är av stor betydelse för alla våra verksamheter. I kommunen hanterar vi varje dag mängder av information som handlar om allt vad vi gör, och rör till exempel skolor, socialtjänst, hemvård, stadsplanering och bygglov. Information kan förekomma i olika former, den kan vara muntlig, skriftlig eller finnas i IT-system. Information är främst i form av texter, men även bilder, symboler, geodata, filmer och ljud utgör information.

Viss information är känslig och måste skyddas från att obehöriga tar del av den. Det handlar ofta om hänsyn till den personliga integriteten och att undvika att enskilda individer kommer till skada. Det finns flera lagar och föreskrifter som kommunen måste leva upp till, samtidigt som privatpersoner, företag och andra har förväntningar och behov på att kommunen hanterar information på ett säkert sätt. Informationssäkerhet handlar om att skapa och upprätthålla lämpligt skydd för att motsvara dessa krav.

Avesta kommun ställer krav på att medarbetare följer dessa riktlinjer för informationssäkerhet. Chefer har ett ansvar att delge information och möjliggöra utbildning i informationssäkerhetsfrågor till sina medarbetare. Om du som medarbetare eller externt kontrakterad har tillgång till känslig information ska du skriva under ett sekretessavtal. Ett sådant avtal gäller även efter att anställningen eller kontraktet upphört.

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

7.1 Skyldighet att rapportera incidenter och brister

Alla medarbetare har skyldighet att rapportera incidenter eller brister som misstänks kunna medföra negativ påverkan på Avesta kommuns information. Det kan röra sig om till exempel:

- IT-angrepp/intrång
- Skadlig kod (till exempel virus)
- Oskyddad känslig information
- Brister i efterlevnad av dessa riktlinjer för informationssäkerhet

IT- och informationssäkerhetsrelaterade incidenter och brister ska rapporteras enligt gällande rutin. Meddela även din chef.

7.2 Säkert beteende

Oavsett om du hanterar information digitalt, muntligt eller i pappersform, är informationssäkerheten 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 menas information som endast får vara tillgänglig för medarbetare som har särskild behörighet att hantera informationen, exempelvis sekretessbelagd information, känsliga personuppgifter, patientjournaler med mera.

Riktlinjer för muntlig information	
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 och i informella sammanhang, till exempel vid fikabordet. Man ska enbart tala i stängda utrymmen och även försäkra sig om att fysiska samtal eller telefonsamtal inte hörs i intilliggande rum.
2.	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.
3.	Digitala möten där information av känslig karaktär avhandlas ska hållas på en av kommunen anvisad särskild plattform där deltagarnas identitet kan säkerställas.

Riktlinjer för information på skärmar och i pappersform	
1.	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.
2.	Konfidentiell information på datorskärmen ska vara skyddad från obehöriga. Skärmen ska låsas och smartkort eller liknande dras ur när man lämnar datorn, även för en kortare stund.
3.	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 rätt.
4.	Vid fysisk posttjänst bör förslutna brev användas för intern information och rekommenderade försändelser bör användas om brev innehåller konfidentiell information.
5.	När konfidentiell information överförs via fax ska man försäkra sig om att man har rätt nummer och att mottagarens fax är övervakad under överföringstillfället. Man ska inte lämna faxen innan överföringen är klar.
6.	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.
7.	Pappersdokument som innehåller konfidentiell information måste vid kassering strimlas eller skickas för förbränning hos godkänd aktör.

7.3 Lösenord

För att logga in i Avesta kommuns IT-miljö krävs tjänstekort och individuell kod. Till flera av IT-systemen du använder i tjänsten krävs dessutom användar-ID och lösenord. Lösenorden är personliga och får inte göras kända för andra. Om en obehörig kommer över ditt lösenord och får tillgång till ditt användar-ID, kan den personen utföra aktiviteter i ditt namn. Användar-ID och lösenord används för att skydda information som kan vara intern eller konfidentiell, och det är därför viktigt att följa nedanstående regler

för skapande och hantering av lösenord. Ett lösenord ska vara ”starkt”, det vill säga svårt att gissa för någon annan. Det ska därför inte kunna förknippas med dig som person och dessutom ha en viss längd och komplexitet. Regler för lösenord beslutas av IT- och digitaliseringschef.

Tips på bra lösenord som är enkla att minnas är att tänka ut en mening. Justera sedan stora och små bokstäver och bilda lösenordet. Exempel:

Mening	Lösenord
Klockan 10 går två bilar till Norrköping!	K10g2btN!

Användar-ID och lösenord är i sig viktig information där användar-ID är intern information medan lösenord är konfidentiell information och ska hanteras på ett säkert sätt:

Riktlinjer för hantering av lösenord	
1.	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.
2.	Olika lösenord ska användas. Samma lösenord ska inte användas privat och i jobbet. Olika lösenord ska dessutom användas för olika tjänster på webben även om de är jobbrelaterade. På så vis minskas riskerna att någon kommer åt information.
3.	Lösenord ska bytas direkt om misstanke finns att det har röjts.
4.	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.
5.	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.

7.4 Enheter

Den IT-utrustning som tillhandahålls av kommunen kan vara stationär eller bärbar, en så kallad mobil enhet. Mobil enhet avser bärbar dator, smarttelefon, surfplatta, USB-minne samt extern hårddisk.

Applikationsspecifika datorer, mobiler eller surfplattor kan ha specifika riktlinjer utöver de som presenteras här. Kolla med din chef om du är osäker vad som gäller.

Riktlinjer för hantering av enheter	
1.	Mobila enheter som tillhandahålls av Avesta kommun är personliga arbetsredskap och får inte lånas eller överlåtas om det inte är enheter som delas av flera.
2.	Uppsatta säkerhetsinställningar i enheter får inte ändras.
3.	Endast godkända programvaror får installeras på enheten.
4.	Installerad programvara får inte kopieras eller installeras på annan enhet.
5.	Mobila enheter ska låsas med lösenord.
6.	Konfidentiell information måste vara krypterad på mobila enheter.

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.
8.	Endast av kommunen godkänd enhet och programvara får anslutas till kommunens nät.
9.	Privat utrustning kan anslutas till kommunens gästnät.
10.	Enheten får enbart anslutas till trådlösa nätverk som är kända och lösenordskyddade.
11.	Vid distansarbete måste utrustning som tillhandahålls från Avesta kommun.
12.	Anslutning med kommunens VPN-anslutning från en privat dator är ej tillåtet.
13.	Försiktighet ska iakttas vid arbete i publika miljöer, exempelvis kan skärmen skyddas med sekretesskydd.
14.	Arbete med konfidentiell information får inte ske i publika miljöer.
15.	Mobila enheter får inte lämnas utan uppsikt och ska förvaras i säkert och skyddat utrymme.
16.	Förlust av enhet ska omedelbart anmälas till IT-supporten, detta ska göras innan polisanmälan. I vissa fall finns möjligheter att fjärradera information.
17.	Vid avslut av anställning eller vid byte till en annan organisatorisk enhet ska mobila enheter återlämnas i enlighet med de rutiner som finns, och får inte behållas privat eller av en verksamhet.
18.	Utrustningen ska i övrigt vårdas och hanteras på det sätt som föreskrivs, till exempel skyddas mot värme och fukt.

7.4.1 Särskilda riktlinjer för smarta telefoner och surfplattor

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

Riktlinjer för smarta telefoner och surfplattor	
1.	Arbetsgivaren 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 möjlighet att ta del av till exempel sms, foton och kalenderanteckningar. Eftersom offentlighetsprincipen gäller kan utomstående begära ut informationen.
2.	Det finns ett stort utbud av appar att ladda ner till den smarta telefonen eller surfplattan. Många appar kan innehålla skadlig kod. I syfte att minska denna risk är det endast tillåtet att ladda ned appar som finns i företagsportalen.
3.	Information som är konfidentiell får inte hanteras i smart telefon eller surfplatta om inte av kommunen godkänd säkerhetslösning används.
4.	Pinkoder, fingeravtryck eller annan autentisering måste användas till smarta telefoner och surfplattor. Då pinkoder används ska inte enkla pinkoder som 0000, 1234 etcetera användas, och inte samma pinkod som används i andra sammanhang.
5.	Vårda utrustningen och använd exempelvis skärmskydd och skal.

7.4.2 Skadlig kod

Skadlig kod är ett samlingsnamn för olika typer av oönskade programvaror som orsakar avsiktlig störning eller skada. I begreppet skadlig kod ingår bland annat virus, trojaner och spionprogram. Dessa kan

installeras på en dator eller ett nätverk utan administratörens samtycke och har utvecklats i syfte att störa IT-system, för att samla in information eller för att utnyttja datorkraft eller minneskapacitet i IT-utrustning.

7.4.3 Spridning av skadlig kod

Skadlig kod kan spridas till en dator eller mobila enhet om man öppnar bilagor i e-post, importerar filer eller klickar på länkar, inklusive sådana som finns i sociala medier. Även hårdvara som USB-minnen kan innehålla skadlig kod.

Identiteter kan kapas, till exempel på Facebook, och e-postadresser kan fejkas i syfte att luramottagaren att klicka på länkar. Webbsidor är inte alltid de som de utger sig för att vara. Vid så kallad phishing luras mottagaren att klicka på en länk som leder till en sida där man ombeds fylla i koder, lösenord eller bankkonton. Var observant på detta och fyll aldrig i sådana uppgifter! Seriösa myndigheter, företag och andra organisationer ber aldrig om uppgifter på detta sätt.

Blir IT-utrustning drabbad av skadlig kod kan det sprida sig vidare i kommunens nätverk och orsaka stor skada.

Kommunens datorer är utrustade med skydd mot skadlig kod. Detta innebär inte fullständig säkerhet då utvecklingen inom detta område är oerhört snabb. Alla medarbetare kan också bidra till ett bra skydd mot skadlig kod genom att följa dessa riktlinjer:

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

7.4.4 Internet och sociala medier

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

Riktlinjer för Internetanvändning	
1.	Internet är främst ett arbetsverktyg och privat användning ska inte störa ordinarie arbetsuppgifter eller innebära merkostnader för kommunen.
2.	Tryckfrihetsförordningen, brottsbalken, lagen om upphovsrätt samt dataskyddsförordningen är exempel på lagar som måste beaktas när man använder Internet.
3.	För material på Internet som ska användas i tjänsten, får nedladdning och installation av upphovsrättsligt material (datorprogram, film, musik, med mera) inte ske utan stöd i lag, avtal eller med skriftligt tillstånd från rättighetsinnehavaren.
4.	I begränsad omfattning får Internet användas för privata syften. Utrymmeskrävande filtyper inklusive filmer, program och spel får dock inte laddas ned, strömmas, lagras eller spridas i, eller via, Avesta kommuns nätverk.

5.	Internet är ett öppet nätverk och endast öppen information får publiceras eller delas, alltså inte intern eller konfidentiell information.
----	--

Uttalanden och andra aktiviteter som görs på Internet kan påverka allmänhetens uppfattning om den enskilde tjänstepersonen som utför aktiviteten och även för Avesta kommun som organisation. Det är därför särskilt viktigt att som representant för Avesta kommun beakta god etik och gott omdöme på Internet.

Etiska riktlinjer	
1.	All kommunikation på Internet från Avesta kommuns datorer ska vara öppen, saklig och etisk, oavsett om kommunikationen sker för privata syften eller inte.
2.	Det är inte tillåtet att besöka webbplatser med till exempel brottslig verksamhet, rasism, diskriminering, extempolitiskt eller pornografiskt innehåll om det inte är nödvändigt för att utföra dina arbetsuppgifter.
3.	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.

Avesta kommun är aktivt på sociala medier. Den personal som skriver i Avesta kommuns namn har särskilda regler och kunskap om kommunikation. Se vidare i *Riktlinje för användning av sociala medier*, som finns att läsa på avesta.se, där finns även information om vad som gäller vid privat bruk.

7.5 E-post

E-post är för många medarbetare det vanligaste och viktigaste sättet att kommunicera internt inom kommunen och till externa parter. Det är dock viktigt att tänka på att kommunikation med e-post normalt är helt öppen. Att skicka e-post som inte är skyddad med till exempel kryptering kan jämföras med att skicka vykort. Se vidare Riktlinjer för e-posthantering för Avesta kommun.

7.6 Lagring och säkerhetskopiering

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

Riktlinjer för lagring och säkerhetskopiering	
1.	Information ska lagras på nätverket så att den säkerhetskopieras. Det kan vara personliga eller gemensamma filer.
2.	Om information behöver lagras på lokal hårddisk, se till att regelbundet kopiera över informationen till nätverket.
3.	Om information har gått förlorad, exempelvis om man av misstag råkat radera ett dokument, ska IT-support kontaktas, förhoppningsvis kan de då återskapa den senaste säkerhetskopian.
4.	Konfidentiell information får endast lagras i godkända system och lagringsytor som har begränsad åtkomst, både vad gäller användare och administratörer av systemet eller lagringsytan.
5.	Lokal lagring av konfidentiell information, till exempel på en persondator, får endast ske om lagringsenheten eller filerna är krypterade av Avesta kommun godkänd metod för kryptering.

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	
1.	Endast godkända molntjänster är tillåtna att användas. Kontrollera vilka molntjänster som är tillåtna inom din verksamhet.
2.	Konfidentiell information får inte lagras i personliga molntjänster.

7.7 Spårbarhet och loggning

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

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

All Internettrafik och e-post loggas centralt. Kommunen kan som arbetsgivare, 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.

8. Informationsklasser

Viss information är mer känslig än annan. Behovet av skydd skiljer sig därför mellan olika typer av information och i olika situationer. Skyddsbehovet beror på legala krav och vilka konsekvenser det skulle få för verksamheten eller för enskilda individer om informationen sprids till obehöriga. I kommunen finns, för information som inte omfattas av säkerhetsskyddslagen, tre klasser för hur känslig informationen är och hur den får spridas: Öppen, Intern eller Konfidentiell. Dessa illustreras i tabellen nedan.

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

Att klassa information på det här sättet är ett arbete som påbörjats i Avesta kommun, men är långt ifrån färdigt. Det viktigaste är att konfidentiell information hanteras på rätt sätt. Konfidentiell information är

bland annat känsliga personuppgifter och sekretessklassad information. Om du är osäker på hur viss information ska klassas och hanteras så fråga din chef.

8.1 Personuppgifter

I de flesta verksamheter hanteras personuppgifter. Dessa måste behandlas enligt gällande författningar som exempelvis dataskyddsförordningen, patientdatalagen och lagen om behandling av personuppgifter inom socialtjänsten.

Hur information som innehåller personuppgifter klassas beror på sammanhang, vilka personuppgifter som avses och så vidare. Känsliga personuppgifter är dock alltid klassade som konfidentiell information. Till känsliga personuppgifter räknas enligt GDPR och dataskyddslagen uppgifter som avslöjar:

- politiska åsikter,
- religiös eller filosofisk övertygelse,
- medlemskap i fackförening,
- personuppgifter som rör hälsa eller sexualliv,
- ekonomisk hjälp eller vård inom socialtjänsten,
- enskilda personliga och ekonomiska förhållanden inom bank- och försäkringsväsendet.

Känsligheten hos personuppgifter beror dock på flera faktorer och även mängden av uppgifter om varje person måste beaktas eftersom den bestämmer hur detaljerad bild av en person som kan skapas. Det innebär att flera personuppgifter som var för sig inte bedöms känsliga tillsammans kan bilda känsliga personuppgifter.

Skyddade personuppgifter är alltid konfidentiell information och ska hanteras utifrån särskilda rutiner och regler.

8.2 Allmänna handlingar och sekretess

En handling är allmän om den är förvarad och inkommen till eller upprättad hos kommunen.

Allmänheten ska kunna ta del av allmänna handlingar och kommunen är skyldig att, efter sekretessprövning, ha tillgång till dessa för att skyndsamt erbjuda den i läsbar form till den som begär det. Information kan vara sekretessbelagd enligt offentlighets- och sekretesslagen. Sådan information får inte lämnas ut och ska klassas som konfidentiell information.

Allmänna handlingar kan vara både i form av analog och digital information och ska hanteras, bevaras och gallras i enlighet med dokumenthanteringsplan.

Arbetsmaterial under ett ärendes beredning, minnesanteckningar för eget bruk, verksamhetsinterna meddelanden och personliga meddelanden är normalt inte allmänna handlingar. Denna information kan klassas som konfidentiell, intern eller öppen information beroende på känslighet, till exempel utifrån lagkrav.

Kapitel C - Informationssäkerhet i verksamhetsnära förvaltning

9. 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.

10. Roller och ansvar

Ansvar 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. Informationssäkerhetsansvarig och övriga som jobbar specifikt med informationssäkerhet fungerar som stöd till kommunens verksamheter i arbetet med att uppfylla informationssäkerhetsansvaret.

Roll	Ansvar
Ledning, kommunfullmäktige, styrelser och nämnder	Har det yttersta ansvaret för informationssäkerheten i den verksamhet som bedrivs inom respektive ansvarsområde.
Förvaltningschef/VD och informationsägare	Ansvarar för informationssäkerheten inom sin verksamhet. Förvaltningschef/VD ansvarar för att medarbetare inom den egna verksamheten har ett säkerhetsmedvetande samt tillräcklig kunskap och förståelse för att nödvändig informationssäkerhet i verksamheten ska uppnås. Informationsägarskap följer verksamhetsansvaret.
System- eller objektägare	Ansvarar för att system eller objekt efterlever policy och riktlinjer för informationssäkerhet. Ansvarar för att systemet och informationen i detta klassas.
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. Systemförvaltaren är normalt en person som arbetar inom den aktuella verksamheten där systemet används och inte en extern funktion på exempelvis IT- och digitaliseringsenheten.

11. 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	
1.	Det ska finnas systemdokumentation för varje IT-system. Dokumentationen består av systemförvaltningsplan, systemsäkerhetsbeskrivning, drift- och användardokumentation.

12. Informationsklassning och systemklassning

Informationsklassning innebär att information klassificeras i olika nivåer utifrån dess skydds krav. Genom att klassa information på detta sätt kan man identifiera känslig och kritisk information så att denna får 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 Avesta kommuns verksamheter.

Klassning av information och system ska ske i SKR:s verktyg KLASSA. Verktöget ska identifiera verksamhetens behov av tekniska och administrativa säkerhets- och skyddsåtgärder för informationen. Verktöget 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

- | | |
|----|---|
| 1. | Data eller information i system eller objekt ska vara inventerad och klassad enligt SKR:s modell för informationsklassning. |
|----|---|

13. Behörighetshantering och loggning

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

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

13.1 Behörighetstilldelning

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

13.2 Ansvar för behörighetstilldelning

Ansvarig chef beställer behörigheter till system. För externa användare gäller att tilldelning av åtkomst även ska vara tidsbegränsad för den tiden som behövs för att utföra uppgiften. Systemägare ansvarar för att tilldela behörigheter.

Varje användare ska ha ett unikt användar-ID, det vill säga gruppidentiteter är generellt inte tillåtna (under vissa förutsättningar kan dock detta beviljas).

13.3 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 skydds krav avseende konfidentialitet och riktighet. Rutiner för behörighetshantering ska följas upp och dokumenteras.

13.4 Logghantering

För att få spårbarhet bör system övervakas och loggas avseende användaraktiviteter, avvikelser, fel och informationssäkerhetsincidenter. Detta är särskilt viktigt, och obligatoriskt, om system hanterar information med höga skydds krav. 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	
1.	Det ska finnas dokumenterade rutiner för hantering av behörigheter och rättigheter till system.
2.	Varje användare ska ha ett unikt användar-ID.
3.	Externa användares åtkomst ska vara tidsbegränsad samt föregås av sekretessavtal.
4.	Det ska finnas dokumenterade rutiner för logghantering i system/objekt.
5.	Höga skydds krav på konfidentialitet, riktighet eller tillgänglighet innebär också höga krav på spårbarhet. Loggning av användares aktiviteter i sådana system är obligatorisk.
6.	Förändringar i anställningar och roller ska omedelbart rapporteras till ansvarig objekt/systemägare så att reglering av behörigheter kan ske.
7.	Uppföljning ska ske av behörighetshantering och logghantering i system/objekt.

14. 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. I kapitel D finns riktlinjer som rör bland annat systemtest och hantering av testdata.

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.

Riktlinjer för ändringshantering	
1.	Det ska finnas dokumenterade processer eller rutiner för hantering av ändringar i system.
2.	Vid avveckling av system ska en plan upprättas för hur information ska migreras, raderas eller slutarkiveras (i enlighet med dokumenthanteringsplan).

15. Användarinstruktioner

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

- Regler kring inloggning och lösenordshantering
- Behörigheter
- Särskilda instruktioner för hur konfidentiell information får hanteras, till exempel känsliga eller skyddade personuppgifter
- Information om vad som loggas och konsekvenser av att bryta mot användar-instruktioner, till exempel att ta del av eller sprida konfidentiell information

- Incidentrapportering – användare ska vara vaksamma på brister och incidenter i systemet och veta hur man ska rapportera dessa
- Eventuell sekretessförbindelse

Riktlinjer för användarinstruktioner	
1.	Informationssäkerhetsregler ska finnas med i användarinstruktioner alternativt hänvisas till.
2.	Det ska finnas särskilda instruktioner för hantering av konfidentiell information som till exempel skyddade personuppgifter.

16. 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. Avesta 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	
1.	Risk- och sårbarhetsanalys ska genomföras i samband med större förändringar i eller omkring system/processer.
2.	Resultat ska dokumenteras. Akuta risker ska tas om hand skyndsamt och återstående åtgärder ska tas med i systemförvaltningsplaner.

17. 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 till exempel 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. Flera fall av mindre incidenter av likadan art kan tillsammans utmytna i eller utgöra en allvarlig incident.

Allvarliga incidenter är större störningar i ett system som till exempel 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-och digitaliseringsenheten.

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	
1.	Det ska finnas rutiner för hur användare ska rapportera incidenter.
2.	Akuta incidenter ska åtgärdas skyndsamt.
3.	Allvarliga incidenter ska utredas och dokumenteras enligt gällande mall.

4.	Allvarliga incidenter som gäller system ska dokumenteras och sammanställas. Kvarstående åtgärdsbehov ska tas om hand i systemförvaltningsplaner.
----	--

18. 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. Det vill säga 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 till exempel genom utbildning av ersättare och systemdokumentation.

Riktlinjer för kontinuitetshantering

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

Kapitel D – Informationssäkerhet i IT- miljön

19. Inledning

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

20. Roller och ansvar

Ansvar för informationssäkerhet och IT-säkerhet inom IT-enheten 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 Avesta kommuns IT-miljö.

20.1 Roller i den IT-nära förvaltningen

20.1.1 IT-säkerhetsansvarig

Den IT-säkerhetsansvarige samordnar arbete med säkerheten i Avesta 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 verksameters 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 Avesta kommuns informationssäkerhetsråd. Den IT-säkerhetsansvarige ska också omvärldsbevaka, nätverka och samverka externt inom området.

20.1.2 Objekt/systemägare

Objekt-/systemägare 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 ansvarar för att Avesta kommuns informationssäkerhetspolicy och dessa riktlinjer efterlevs och ska utse systemförvaltare för objekt/system.

20.1.3 Teknisk systemförvaltare

Teknisk systemförvaltare samverkar med användarna i verksamheterna och i ser till att IT-säkerhetsrelaterade mål och åtgärder i objekt/system nås samt genomförs.

20.1.4 IT-tekniker

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

21. Hantering av tillgångar

21.1 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- och digitaliseringschef är ansvarig.

21.2 Klassning av IT-resurser

IT-resurser ska klassas i enlighet med SKR:s modell för informationsklassning. Underliggande IT-resurser i form av infrastruktur, stödsystem med mera 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.

21.3 Instruktioner för användare

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 skydds krav. 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, till exempel hur åtkomst till nätverk får ske, hur nätverkstjänster får användas, hur autentisering ska ske och hur utrustning som ansluts till nätverk ska identifieras
- Operativsystem, till exempel hur åtkomst och autentisering ska ske
- Klientdatorer, till exempel regler för programinstallationer som utförs av användare

Riktlinjer för hantering av tillgångar

1.	Samtliga IT-resurser ska identifieras och tilldelas en ägare med rollerna objekt-/systemägare
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.

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

22. 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, till exempel 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 man kan göra med den, till exempel läsa, skriva, ändra, radera
- Loggning av användarens aktiviteter.

22.1 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, det vill säga verifiering av en uppgiven identitet. Vid åtkomst till information med höga skydds krav avseende konfidentialitet och/eller riktighet ska stark autentisering användas. Som stark autentisering räknas identifiering av en person och verifiering av personens autenticitet genom en kombination av minst två tekniska lösningar (tvåfaktorsinloggning).

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 till exempel från administratör eller handläggare oavsett om lösenordet tilldelas, förändras eller återställs.

Riktlinjer för identifiering och autentisering	
1.	Alla användare ska ha en unik användaridentitet.
2.	Namn på användare, som underlag för till exempel e-postadresser, ska vara enhetliga i kommunen och stämma överens med folkbokföringen. Särskilda skäl för undantag kan finnas, exempelvis skyddade identiteter.
3.	Vid åtkomst till information med höga skydds krav avseende konfidentialitet eller riktighet ska stark autentisering användas.
4.	Fjärråtkomst för inloggning med konton med höga behörigheter till IT-resurs med höga skydds krav avseende konfidentialitet eller riktighet är inte tillåten.
5.	Lösenord är alltid konfidentiell information som har höga skydds krav och ska i alla skeden av sin livscykel skyddas mot åtkomst från alla andra än ägaren själv. För att minska risken för obehörig åtkomst ska följande skyddsfunktioner införas: <ul style="list-style-type: none"> • Tekniska funktioner implementeras där så är möjligt i IT-resursen för att säkerställa att lösenordsregler för medarbetare avseende historik, komplexitet och åldring av lösenord följs. • Lösenord ska aldrig skickas/transporteras i klartext över nätverk. I de fall detta inte är möjligt ska tillfälliga lösenord i kombination med tvingande lösenordsbyte användas. Tillfälliga lösenord ska enbart vara giltiga för en (1) inloggning. • Lösenord får aldrig lagras på ett sätt som gör det möjligt att dekryptera dem till klartext. Om felaktigt lösenord används mer än tre gånger ska aktuellt användar-ID utestängas en viss tid ur systemet och händelsen loggas.
6.	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.

22.2 Reglering av åtkomsträttigheter

Åtkomst till IT-resurser ska baseras på dess klassning, exempelvis ställs större krav på metoder för autentisering vid åtkomst till information med höga skydds krav. 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 ansvarar för att upprätta ett behörighetskontrollsystem som motsvarar dessa krav. Det ska finnas beslutade och dokumenterade regler och rutiner för behörighetshantering, det vill säga 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 behörighetshandlingen, till exempel 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 åtkomstilldelning, även ska vara tidsbegränsad för endast den tiden som behövs för att utföra uppgiften samt föregås av sekretessavtal.

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

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

Riktlinjer för reglering av åtkomsträttigheter	
1.	Det ska finnas beslutade och dokumenterade regler och rutiner för behörighetshandling för IT-resurser.
2.	IT-resurser ska ha åtkomsträttigheter som motsvarar hur de är klassade.
3.	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.
4.	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.
5.	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.
6.	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 till exempel omfatta en installation av programvara och i andra hand ges för en viss tid med ett specifikt slutdatum. Objekt-/systemägare beslutar om tilldelning av privilegierad åtkomsträtt. Granskning av administrativa rättigheter ska ske i enlighet med verksamhetens behov och legala förutsättningar.
7.	Gruppidentiteter är inte tillåtna. Eventuella undantag ska godkännas av systemägare verksamhet. Gruppidentiteter ska då enbart beviljas under följande förutsättningar: <ul style="list-style-type: none"> • Behov av gruppidentitet är tydligt beskrivet och alternativen utredda så att det framgår varför gruppidentiteten är nödvändig • Gruppidentiteten ska ha en registrerad ägare • Gruppidentiteten ska vara tidsbegränsade med tydligt slutdatum • En avvecklingsplan ska finnas för att ersätta gruppidentiteten med individuella identiteter • Ägaren av gruppidentiteten ska föra en förteckning alla som använder identiteten. • Historikfunktion ska finnas så att förteckningen kan visa vilka användare som fanns viden given tidpunkt • Användande av gruppidentiteter ska dokumenteras enligt ovan. • Autentiseringsinformation ska uppdateras om någon användare lämnar gruppidentiteten. Om en användare till exempel lämnar en gruppidentitet med ett delat lösenord så ska lösenordet ändras och ett nytt lösenord distribueras till kvarvarande användare av gruppidentiteten • Ägaren av gruppidentiteten tar fullt ansvar för eventuellt missbruk av gruppidentiteten
8.	För externa användare gäller att tilldelning av åtkomst, utöver övriga regler för åtkomstilldelning även ska: <ul style="list-style-type: none"> • Tidsbegränsas att endast omfatta tiden som behövs för att utföra uppgiften • Föregås av sekretessavtal

22.3 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	
1.	Vid åtkomst till IT-resurs och information med höga skydds krav avseende konfidentialitet eller riktighet krävs loggning av åtkomst för att erhålla spårbarhet.
2.	Loggningsverktyg och logginformation ska skyddas mot manipulation och obehörig åtkomst, logginformation innehållande loggning av åtkomst har alltid höga skydds krav avseende konfidentialitet eller riktighet.
3.	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.

22.4 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 skydds krav på konfidentialitet och/eller riktighet.

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

Ibland kan krypteringslösningar medföra nya risker relaterade till nyckelhantering. Dessa risker behöver hanteras bland annat genom återkallande, validering och återställning av nycklar:

- Återkallande 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 till exempel 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	
1.	Krypteringslösningar ska baseras på etablerade standarder och införande ska godkännas av informationssäkerhetsrådet.
2.	Nyckelhantering ska säkerställas för att tillgodose de krav som finns för IT-resurs avseende: <ul style="list-style-type: none"> • Återkallande av nycklar • Validering av nycklars giltighet och autenticitet • Återställning av nycklar
3.	Krypteringsnycklar är konfidentiell information och ska skyddas därefter.

23. 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.

23.1 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 etcetera. VA-dragningar i eller i direkt närhet av driftmiljö ska undvikas och risker för vatteninträngning hanteras. Om golvbrunn finns ska åtgärder vidtas för att undvika att vatten kan tränga upp. Godkänt brandskydd och brandlarm ska finnas. Släckutrustning ska väljas så att inte onödiga skada uppstår vid släckning av brand. Ventilation och andra genomföringar mellan brandceller ska förses med brandspjäll.

Säkra utrymmen som innehåller IT-resurser med höga skydds krav ska bevakas och fysisk närvaro ska loggas (till exempel tillträdes- eller videoövervakningsloggar).

23.2 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.

23.3 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 skydds krav 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.

23.4 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 (till exempel 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.

23.5 Elförsörjning

Säker elförsörjning (till exempel avbrottsfri kraft genom UPS (uninterruptible power supply) 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	
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.
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.
3.	Beslut om vem som ges tillträde att arbeta i säkra utrymmen ska vara dokumenterat.
4.	Personal som beviljats tillfälligt tillträde till säkra utrymmen ska övervakas under hela besöket.
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.
6.	Inkommande gods ska registreras och godkännas av egen personal vid leveranstillfället och eventuella avvikelser från förväntad leverans ska kvitteras av leverantören.
7.	Godkänt brandskydd och brandlarm ska installeras. Släckutrustning ska väljas så att inte onödig skada uppstår vid släckning av brand. Ventilation och andra genomföringar mellan brandceller ska förses med brandspjäll.
8.	Utrymmet ska utformas så att utrustningen inte utsätts för vätskeläckage, korrosiva brand- och släckgaser, damm etcetera. VA-dragningar i eller i direkt närhet av driftmiljö ska undvikas och risker för vatteninträning hanteras. Om golvbrunn finns ska åtgärder vidtas för att undvika att vatten kan tränga upp.
9.	Utrymmen som innehåller informationstillgångar med höga skydds krav ska uppfylla Skyddsklass 3 enligt SSF 200 Inbrottskydd.
10.	IT-resurser ska skyddas från elavbrott och andra störningar som orsakas av fel i tekniska försörjningssystem.
11.	Kablage för ström och telekommunikation för data eller stödjande informationstjänster ska skyddas från avlyssning, störningar och skada.
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.
13.	Datamedia som innehåller för verksamheten kritisk information och systeminformation ska förvaras i för datamedia brandskyddsklassat datamedieskåp.
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 skydds krav ska sekretessavtal tecknas. Vid känslig information döljas, flyttas eller raderas från utrustningen. Underhåll och reparation ska följas upp i loggböcker.
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 förstörs.

16.	Avveckling eller skrotning av datamedia med höga skydds krav på konfidentialitet sker genom att information skrivs över i multipla operationer, alternativt att mediet där informationen lagrats förstörs på ett fullständigt och oåterkalleligt sätt. Observera att krypterad datamedia inte är känslig om nyckel för dekryptering ges ett fortsatt skydd, eller att nyckel destruerats.
17.	IT-utrustning ska inte avlägsnas utanför kommunens lokaler utan tillstånd.
18.	IT-utrustning tillhörande kommunen avsedd att användas utanför kommunens lokaler ska förses med stöldskydd och märkning.

24. Driftsäkerhet

24.1 Driftsrutiner

Det ska finnas dokumenterade driftsrutiner tillgängliga för alla användare som behöver dem. Driftsrutiner ska vara formella och beslutade dokument och utgör en 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	
1.	Det ska finnas formella, beslutade och dokumenterade driftsrutiner för väsentliga processer och objekt. Dessa ska göras tillgängliga för alla användare som behöver dem.
2.	Ändringar i IT-resurser ska följa fastställd process som säkerställer att ändringarna är riskbedömda, planerade, kommunicerade, testade och godkända.
3.	Utvecklings-, test- och driftmiljöer ska vara separerade för att minska risken för obehörig åtkomst eller ändringar i driftmiljön.

24.2 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 skydds krav ska regelbundet granskas med avseende på skadlig kod. Om angrepp av skadlig kod inträffat ska det finnas en fastställd rutin för återställning av IT-resurser. Det ska finnas rutiner för att regelbundet samla in information om skadlig kod.

Riktlinjer för skydd mot skadlig kod	
1.	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.
2.	Alla datorer (servrar och klienter) ska ha skydd mot skadlig kod (antivirusprogramvara) som frekvent och regelbundet uppdateras (dagligen)
3.	IT-resurser som stöder objekt med höga skydds krav ska regelbundet granskas med avseende på skadlig kod.
4.	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
5.	Det ska finnas en fastställd rutin för återställning av datorer om kommunen skulle drabbas av skadlig kod eller virusutbrott.
6.	Det ska finnas rutiner för att regelbundet samla in information om skadlig kod, till exempel prenumerera på nyhetstjänster eller bevaka webbplatser som ger information om ny skadlig kod.

24.3 Säkerhetskopiering

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

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.

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

Riktlinjer för säkerhetskopiering	
1.	För IT-resurser med höga skydds krav avseende tillgänglighet ska redundans finnas i delkomponenter, system, lagring och nätverk samt säkerställd infrastruktur för IT-drift, till exempel UPS elförsörjning, reservkraft, redundant kyla med mera. 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.
2.	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

	<p>omfattas av säkerhetskopiering, hur lång tid som säkerhetskopior ska sparas samt vilka kontroller som ska genomföras av att säkerhetskopiorna fungerar. Vidare ska maximal informationsförlust och målsättning för återställningstid definieras för varje IT-resurs och tillsammans med övriga krav ligga till grund för vald backuplösning.</p> <ul style="list-style-type: none"> • Målsättning för återställning av data, RPO (Recovery Point Objective), den maximalt acceptabla mängden av dataförlust som tillåts vid en återställning av en IT-tjänst efter ett avbrott ska fastställas • Målsättning för återställningstid, RTO (Recovery Time Objective), den längsta acceptabla tiden för att återställa IT resursen efter ett avbrott ska fastställas
3.	Det ska finnas en process för återlagring från säkerhetskopior som är testad och dokumenterad för respektive IT-resurs.
4.	Backup av IT resurser med höga skydds krav avseende tillgänglighet (höga RTO krav) bör lagras på snabbt backupmedia. Övervakning av backupfunktion ska konfigureras med automatlarm vid problem.
5.	Säkerhetskopiering av information med höga skydds krav avseende konfidentialitet ska ske till krypterad backupmedia eller ges motsvarande skydd. Säkra återställningsrutiner ska användas med kontroller att återställning av konfidentiell information ges rätt skydd efter återställning, till exempel bör dekryptering under återställning undvikas.
6.	Säkerhetskopior ska lagras geografiskt åtskilt från originalmaterialet. Om lösning används där man skiljer på långtids- och korttidslagring är det tillräckligt att långtidslagringen är skild från originalmaterialet under förutsättning att korttidslagrade säkerhetskopior förvaras i ett säkert utrymme avsett för datamedia.

24.4 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 informationssäkerhetskändelser 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

1.	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.
2.	För att säkerställa all typ av loggning av händelser ska systemklockorna i alla relevanta IT-resurser synkroniseras mot en betrodd referenskälla för korrekt tid.
3.	Loggningsverktyg och logginformation har höga skydds krav och ska skyddas mot manipulation och obehörig åtkomst.

24.5 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 vilket sätt.

Riktlinjer för hantering av tekniska sårbarheter	
1.	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.
2.	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.
3.	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 till exempel bestå av skanning av sårbarheter med automatiserade verktyg eller så kallade penetrationstester.
4.	Det ska finnas regler för programinstallationer som utförs av användare som definierar vilka typer av program en användare kan installera och på vilket sätt.

25. Kommunikationssäkerhet

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

25.1 Nätverkssäkerhet

Det ska finnas rutiner för hantering av nätverk. Förvaltning ska ske av ansvariga som utpekats 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	
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.
2.	Trådlös datakommunikation innehållande information med normala eller höga skydds krav avseende konfidentialitet är endast tillåtet från godkända klienter. Teknik för att kryptera och säkra kommunikationen ska alltid användas oavsett skydds krav.
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. <ul style="list-style-type: none"> • Utrustning ska finnas för att kontrollera och förhindra obehörig nätverkstrafik mellan olika nätverkssegment.
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.
5.	Kommunikationstjänster mellan Avesta kommun och externa nätverk ska dokumenteras och godkännas av objekt-/systemägare innan inkoppling får ske.

25.2 Informationsöverföring

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

Avtal som reglerar säker överföring av information mellan Avesta kommun och extern part ska upprättas. Användandet av osäkra klartextprotokoll som till exempel FTP och HTTP ska undvikas och ersättas av säkra alternativ om information med normala eller höga skydds krav avseende konfidentialitet ska överföras.

Riktlinjer för informationsöverföring	
1.	Kommunikation med höga skydds krav avseende konfidentialitet och riktighet ska alltid krypteras och kommunicerande parter ska identifieras på ett säkert sätt med digitala signaturer eller motsvarande.
2.	Utgående massutskick av e-post ska begränsas för att förhindra att kapad mailbox används till att skicka ut stora mängder spam.
3.	Överföringslösningar för information mellan Avesta kommun och externa parter ska regleras genom avtal där minst följande regleras: <ul style="list-style-type: none"> • Motparten informeras om informationens klassning och garanterar att information med normala eller höga skydds krav avseende konfidentialitet ges rätt nivå av skydd och inte förs vidare till annan part. • Kommunikationslösning ska definieras med de nätverkskomponenter som ingår i säkerhetslösningen samt den konfiguration och de inställningar som krävs för att upprätthålla rätt nivå av skydd. • Vid kommunikation med annan part med normala eller höga skydds krav avseende konfidentialitet ska överföringen skyddas med kryptering. • Trafik i uppsatta förbindelser ska om möjligt loggas av båda parter.

4.	Kommunikation med e-post till andra organisationer skyddas i samtliga e-postsystem genom att konfigurera och aktivera standardiserade säkerhetsfunktioner.
----	--

26. Anskaffning och utveckling av IT-resurser

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

26.1 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 (till exempel anpassning av ett inköpt standardssystem).

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

Utveckling, anskaffning eller förändring av system som omfattas av verksamhetsnära förvaltning ska involvera parterna i förvaltningsorganisationen. Objekt-/systemägare 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 med mera ska ha minst motsvarande krav som de system som de stöder. Ibland kan kraven vara ännu högre än för de system de stödjer, exempelvis om en IT-resurs stödjer ett stort antal system som var för sig inte är kritiska.

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

Riktlinjer för säkerhetskrav på IT-resurser

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 (till exempel anpassning av ett inköpt standardssystem). 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.

26.2 Säkerhetskrav vid upphandling av IT-stöd

Vid upphandling av IT-stöd gäller ovanstående riktlinjer för säkerhetskrav på IT-resurser. Det är viktigt vid upphandling att vara tydlig när det gäller kravställning av informationssäkerhet. Leverantörer använder kanske annan terminologi och har annan förståelse för informationssäkerhet än vad som finns 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 implementering 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 (till exempel certifieringar)
- Leverantörens kontinuitetsshantering
- Rätt till tredjepartsrevision

- Sekretessavtal
- Personuppgiftsbiträdesavtal
- Säkerhetsskyddsavtal
- Rätt till incidentrapporter från leverantören som berör leveranser till Avesta 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 IT- och digitaliseringsenheten.

Riktlinjer för säkerhetskrav vid upphandling av IT-stöd	
1.	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.
2.	IT-leverantörer ska alltid delge hur de bedriver säkerhetsarbete i både den operativa verksamheten och i arbetet med systemutveckling.
3.	Avtal med IT-leverantör ska innefatta stöd och support i händelse av fel och incidenter.
4.	Avtal med IT-leverantör ska innefatta: <ul style="list-style-type: none"> • Att leverantören innan leverans till Avesta kommun genomför säkerhetstestning av system och ingående komponenter.
5.	Att leverantören ska åtgärda eventuella säkerhetsbrister som identifierats i samband med acceptanstest och/eller leveranskontroll.
6.	Avtal med IT-leverantör ska reglera hur kontroll av avtalets uppfyllande ska ske, till exempel genom tredjepartsrevision eller granskning genomförd av Avesta kommun.
7.	Upphandling av system som ska driftas hos extern leverantör medför ytterligare krav, exempelvis: <ul style="list-style-type: none"> • Fördjupade krav på leverantörens interna IT-miljö och informationssäkerhet (till exempel certifieringar) • Leverantörens kontinuitetshantering • Rätt till tredjepartsrevision • Sekretessavtal • Personuppgiftsbiträdesavtal • Rätt till incidentrapporter från leverantören som berör Avesta kommun •
8.	Upphandling av IT-stöd ska göras i samverkan med upphandlingsenheten.
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: <ul style="list-style-type: none"> • Hur applicerbara krav i avtal med IT-leverantör säkerställs även mot dess underleverantör • Hur rättsliga krav uppfylls, exempelvis rörande lagstiftning om sekretess och personuppgifter • Vilka åtgärder som vidtas för att säkerställa att alla berörda parter, inklusive underleverantörer, är medvetna om sitt säkerhetsansvar, licensieringsarrangemang, äganderätt till koden och upphovsrätt • Vilka åtgärder som vidtas för att säkerställa kvaliteten i leverans från underleverantör

26.3 Säkerhet vid systemutveckling

Regler för säker utveckling av program och system ska upprättas och tillämpas vid systemutveckling. 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	
1.	Processer, rutiner och regler ska finnas som reglerar att informationssäkerhet finns med under hela utvecklingscykeln av IT-resurser.
2.	För systemutvecklings- och integrationsåtgärder ska utvecklingsmiljöer upprättas och skyddas över IT- resursens hela livscykel.
3.	Systemutvecklare ska ha kompetens i programvarusäkerhet.
4.	Outsourcad systemutveckling ska övervakas och styras efter behov.

26.4 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, till exempel verktyg för kodgranskning eller för skanning av sårbarheter. Testning bör utföras i en realistisk testmiljö för att säkerställa att systemet inte kommer att införa sårbarheter i organisationens miljö och att testerna är tillförlitliga.

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

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

Riktlinjer för säkerhetskrav vid test	
1.	Säkerhetsfunktionalitet ska testas vid utveckling och testning ska göras gentemot de ställda säkerhetskraven och i enlighet med överenskommen säker utveckling.
2.	Produktionsdata ska inte användas i test utan all testdata ska väljas ut noggrant, skyddas och styras. Om produktionsdata ändå behöver används gäller följande: <ul style="list-style-type: none"> • Testdata ska alltid anonymiseras från personuppgifter • Rutiner för styrning av åtkomst som tillämpas för produktionssystem ska också gälla vid test av sådana system • Behörighet ska godkännas av objekt-/systemägare varje gång produktionsdata kopieras till ett testsystem • Produktionsdata ska omgående raderas från testsystem efter avslutad test • Kopiering av produktionsdata ska loggas för att erhålla spårbarhet.
3.	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.

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

Incidenter drivs av objekt-/systemägare, IT-avdelning och övriga berörda parter är delaktiga i lösning av problemet. Incidenter där brott eller misstanke om brott finns ska alltid polisanmälas och insamling av bevis med mera ska inte göras utan samråd med polisen. Medarbetare och deltagare i verksamheten som har upptäckt en incident eller svaghet där brott misstänks föreligga, ska inte själva försöka bevisa brott 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, till exempel genom incidentrapporter och statistik, ska ligga till grund för framtida beslut för att förbättra skyddet, till exempel att investera i nya säkerhetslösningar.

Riktlinjer för incidenthantering	
1.	Det ska finnas en incidenthanteringsprocess som omfattar informationssäkerhetsincidenter. Processen ska innefatta: <ul style="list-style-type: none"> • Mottagning av information om incidenten • Styrning av eventuella behov av omedelbara åtgärder. Dessa kan vara av 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 av eller involverade i återställandet till normal drift.
2.	Större incidenter ska sammanställas i incidentrapporter som respektive objekt-/systemägare ansvarar för att ta fram i samverkan med IT-avdelningen.
3.	Erfarenheter från inträffade incidenter, till exempel genom incidentrapporter och statistik, ska ligga till grund för framtida beslut för att förbättra skyddet, till exempel att investera i nya säkerhetslösningar.
4.	Medarbetare är skyldiga att rapportera informationssäkerhetsincidenter såväl som informations- och IT-relaterade brister i system eller tjänster.
5.	Incidenter där brott eller misstanke om brott föreligger ska alltid polisanmälas.

28. 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 bland annat krisorganisation, kontaktpersoner och operativa steg att vidta under en allvarlig störning eller kris.

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

28.1 Kontinuitetshantering

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

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

Riktlinjer för kontinuitetshantering	
1.	Det ska finnas kontinuitetsplaner för samtliga kritiska IT-resurser med höga skydds krav avseende tillgänglighet.
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.
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.

29. 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 Avesta kommuns informationssäkerhet i stort kan även omfatta IT-miljön.

Riktlinjer för granskning och kontroll	
1.	Kritiska delar i IT-miljön som stödjer objekt med höga skyddsvärden ska regelbundet övervakas och granskas för att sårbarheter och brister ska upptäckas.
2.	Nya IT-lösningar ska vid minsta osäkerhet gällande säkerhetsförhållanden utsättas för tekniska granskningar.
3.	Sårbarheter och brister som upptäcks vid granskningar ska tas upp för åtgärdande i genomförandeplaner. Akuta sårbarheter och brister ska åtgärdas omedelbart.
4.	Rapportering av större sårbarheter och brister ska ske till informationssäkerhetsrådet.
5.	Revision av hela eller delar av IT-miljön ska göras minst vartannat år. Innan granskning eller revision kan ske ska följande beaktas: <ul style="list-style-type: none">• Behov på åtkomst till system och data inför granskning eller revision ska avtalas med 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 till skrivskyddad 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