HÖGSBY KOMMUN

# RIKTLINJER FÖR INFORMATIONSSÄKERHET


SAMMANFATTNING

Riktlinjer för informations-säkerhet syftar till att beskriva ”Vad” som ska göras för att uppfylla ledningens viljeyttring, vilket framgår av den av kommunfullmäktige beslutade informationssäkerhetspolicyn.



Jonas Högquist,
Informationssäkerhets- och utvecklingsstrateg


| Dokumenttyp | Dokumentnamn | Beslutad/Antagen | Version |
|---|---|---|---|
| Riktlinje | Riktlinjer för informationssäkerhet Högsby kommun | KS 2022-01-18 (KS § 7 KU.2021.404) | 1.0 |
| **Dokumentägare** | **Dokumentansvarig** | **Reviderad** | **Giltighetstid** |
| Kommunstyrelsen | Informationssäkerhets- och utvecklingsstrateg | | 2022–2024 |

# Innehåll


1 Inledning ..... - 1 -

1.1 Beskrivning av informationssäkerhet ..... - 1 -

1.2 Mål ..... - 2 -

1.3 Syfte och omfattning ..... - 2 -

1.4 Grunder ..... - 2 -

1.5 Lagar och regler ..... - 3 -

1.6 Högsby kommuns övergripande styrdokument ..... - 3 -

1.7 Revision och ständig förbättring ..... - 4 -

2 Termer och definitioner ..... - 5 -

3 Riskbedömning och riskhantering ..... - 2 -

4 Organisation ..... - 2 -

4.1 Roller och ansvar inom den politiska ledningen ..... - 2 -

4.2 Roller och ansvar i verksamheten ..... - 3 -

4.3 Övriga roller ..... - 3 -

4.4 Roller och ansvar gällande samordning och uppföljning ..... - 4 -

5 Personalresurser och informationssäkerhet ..... - 5 -

5.1 Före anställning ..... - 5 -

5.2 Under anställning ..... - 6 -

5.3 Avslut eller ändring av anställning ..... - 8 -

6 Hantering av tillgångar ..... - 8 -

6.1 Förteckning över informationstillgångar ..... - 9 -

6.2 Ägarskap av tillgångar ..... - 9 -

6.3 Klassificering av information ..... - 9 -

6.4 Hantering av tillgångar ..... - 10 -

6.5 Hantering av sekretessbelagd information ..... - 10 -

6.6 Bevarande, rensning och gallring av information ..... - 10 -

6.7 Personuppgifter ..... - 11 -

6.8 Skyddade personuppgifter ..... - 11 -

7 Användning av IT-system ..... - 11 -

7.1 Generella regler för användning av Högsby kommuns IT-system ..... - 11 -

7.2 Anslutning av utrustning i Högsby kommuns IT-system ..... - 12 -

7.3 Användning av Högsby kommuns IT-system ..... - 12 -

7.4 Privat användning av Högsby kommuns IT-system ..... - 13 -

7.5 Användning av Internet ..... - 13 -

7.6 Användning av e-post ... - 14 -
7.7 Användning av sociala medier ... - 15 -
7.8 Användaridentiteter, lösenord och e-tjänstekort ... - 15 -
7.9 Kontrollåtgärder ... - 15 -
8 Åtkomst till information ... - 16 -
8.1 Styrning av åtkomst till elektronisk information ... - 16 -
8.2 Extern informationsanvändning ... - 20 -
8.3 Styrning av åtkomst till icke digital information ... - 20 -
9 Kryptering ... - 21 -
9.1 Kryptografiska säkerhetsåtgärder ... - 21 -
10 Driftsäkerhet ... - 23 -
10.1 Generella krav på systemmiljö ... - 23 -
10.2 Systemförvaltning ... - 23 -
10.3 Systemdokumentation ... - 24 -
10.4 Säkerhetsuppdateringar ... - 24 -
10.5 Skydd mot skadlig kod ... - 24 -
10.6 Styrning av ändringar i eller kring IT-system ... - 25 -
10.7 Felhantering ... - 25 -
10.8 Kapacitetsplanering ... - 25 -
10.9 Säkerhetskopiering och återläsning av data ... - 26 -
10.10 Driftövervakning ... - 26 -
10.11 Drift hos extern part ... - 27 -
10.12 Gallring av information och avveckling av IT-system ... - 28 -
11 Kommunikations- och nätverkssäkerhet ... - 28 -
11.1 Säkerhetskrav på nätverksmiljön ... - 28 -
11.2 Särskilda riktlinjer för trådlösa nätverk ... - 29 -
12 Utveckling och anskaffning av IT-system ... - 29 -
12.1 Generella regler vid utveckling och anskaffning ... - 29 -
12.2 Systemutvecklingsprojekt ... - 30 -
12.3 Upphandling av IT-system och systemutveckling ... - 30 -
13 Leverantörsrelationer ... - 31 -
13.1 Informationssäkerhet i leverantörsrelationer ... - 31 -
14 Fysisk och miljörelaterad säkerhet ... - 32 -
14.1 Generella regler för fysisk och miljörelaterad säkerhet ... - 32 -
14.2 Säkra utrymmen ... - 32 -

14.3 Utrustning och skydd ..... - 33 -
14.4 Kraftförsörjning och elmiljö ..... - 33 -
14.5 Säkerhet för tillgångar utanför egna lokaler ..... - 34 -
15 Hantering av incidenter som rör informationssäkerhet ..... - 34 -
15.1 Incidenthantering ..... - 34 -
16 Kontinuitetsplanering ..... - 37 -
16.1 Generella regler för kontinuitetsplanering ..... - 37 -
16.2 Redundans ..... - 37 -
17 Uppföljning och efterlevnad ..... - 38 -
17.1 Uppföljning av regelverket ..... - 38 -
17.2 Uppföljning av efterlevnad ..... - 38 -

# 1 Inledning

Högsby kommuns verksamhet är omfattande och komplex, med många olika intressenter och med ett stort beroende av information. En effektiv och säker användning av information är en förutsättning för Högsby kommuns verksamhet. Informationssäkerhetsarbetet främjar verksamheternas funktionalitet, kvalitet och effektivitet och tillgodoser invånarens rättigheter och personliga integritet. Sammantaget är detta viktiga förutsättningar för att skapa förtroende avseende vår förmåga att leverera service till våra invånare.

Dessutom ställer offentlighetsprincipen krav på Högsby kommuns informationshantering, liksom speciallagstiftning inom verksamhetsområden som hälso- och sjukvård. Detta sammantaget gör information till en av Högsby kommuns mest betydelsefulla resurser.

Informationssäkerhet handlar om kvalitet och att den är en förutsättning för att uppnå exempelvis säkerhet och integritet för våra medborgare, företag och föreningar. Att förbättra en verksamhets informationssäkerhet innebär inte enbart att tillmötesgå externa krav, utan även att förbättra verksamheten i sig, ett sätt att uppnå god kvalitet och god intern kontroll.

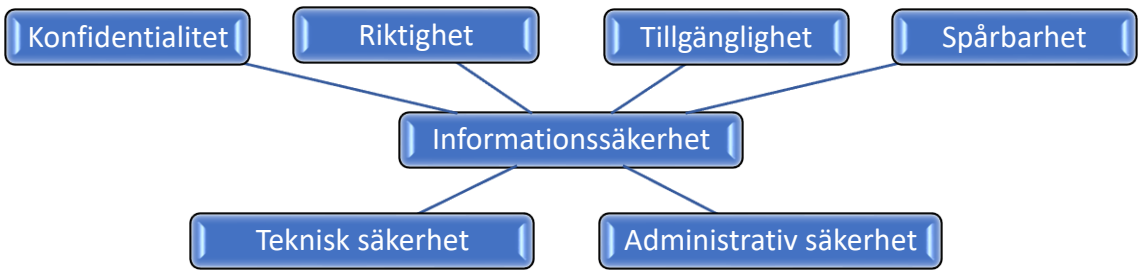
Informationssäkerhetsarbetet berör hela Högsby kommuns verksamhet, varför ett sunt och vaket säkerhetsmedvetande hos alla medarbetare är en förutsättning för väl fungerande informationssäkerhet.

Dessa riktlinjer för informationssäkerhet utgår från allmänt vedertagna säkerhetsstandarder och specifikt standarden SS-EN ISO/IEC 27002:2017 som är utgiven av standardiseringsorganisationerna SIS – Svenska Institutet för Standarder samt CEN (Comité Européen de Normalisation - europeisk standardisering) och ISO (International Organization for Standardization - internationell standardisering), och riktar in sig på de objekt som ska skyddas.

## 1.1 Beskrivning av informationssäkerhet

Informationssäkerhet omfattar skydd av all information oavsett form och innebär en strävan att skydda information så att:

- endast behöriga personer får ta del av informationen (konfidentialitet),
- informationen går att lita på, att den är korrekt och inte manipulerad (riktighet),
- informationen finns tillgänglig när den behövs (tillgänglighet) samt
- att hanteringen av informationen i väsentliga delar är spårbar (spårbarhet).



Konfidentialitet, riktighet, tillgänglighet och spårbarhet utgör informationens egenskaper. Behovet av skydd utgörs av åtgärder som kan vara både av teknisk och administrativ natur.

Exempel på tekniska säkerhetsåtgärder är IT-säkerhet, fysisk säkerhet och datakommunikation, medan administrativ säkerhet är dokumentation, processer, analys, organisation, kompetensutveckling, efterlevnad, uppföljning samt ledning och styrning.

## 1.2 Mål

Målet för Högsby kommuns informationssäkerhetsarbete är att skydda informationen inom verksamheten. Skyddet ska vara anpassat till skyddsvärde, risk och lagkrav och därigenom möjliggöra för Högsby kommuns verksamheter att uppnå sina mål. En god informationssäkerhet inom Högsby kommun främjar verksamheternas funktionalitet, kvalitet och effektivitet, medborgares rättigheter och personliga integritet, Högsby kommuns förmåga att förebygga och hantera allvarliga störningar och kriser samt förtroendet för Högsby kommuns informationshantering och IT-system.

## 1.3 Syfte och omfattning

Dessa riktlinjer, vilka är en konkretisering av Högsby kommuns informationssäkerhetspolicy, är tillsammans med tillhörande tillämpningsanvisningar och instruktioner, styrande för Högsby kommuns informationshantering.

Riktlinjerna gäller för all verksamhet inom kommunen inklusive helägda bolag och omfattar alla informationstillgångar som kommunen hanterar.

Samtliga anställda, extern personal och politiker som aktivt arbetar i verksamheten omfattas av informationssäkerhetspolicyn med dess tillhörande riktlinjer och instruktioner. Övriga, t ex politiker och elever som ges tillgång till kommunens IT-nätverk omfattas också av riktlinjerna.

Med informationstillgång avses all information oavsett om den behandlas i ett IT-system, förkommer på ett utskrivet papper, i ett anteckningsblock, som ett samtal i korridoren eller i telefonen. Även film, ljud och bild inkluderas.

## 1.4 Grunder

Inom Högsby kommun ska ett systematiskt och långsiktigt informationssäkerhetsarbete bedrivas.

Högsby kommuns informationstillgångar ska identifieras, klassificeras och ges en lämplig skyddsnivå med utgångspunkt i att de finns tillgängliga när de behövs (tillgänglighet), att de är korrekta (riktighet), att obehöriga inte kan få tillgång till dem (konfidentialitet) och att händelser i informationsbehandlingen kan spåras (spårbarhet).

Högsby kommuns verksamheter ska, utifrån återkommande risk- och sårbarhetsanalyser och inträffade incidenter, avgöra hur risker ska hanteras och vidta nödvändiga åtgärder för att upprätthålla rätt skyddsnivåer för informationen.

För att uppnå målet med informationssäkerheten ska säkerhetsarbetet omfatta samtliga delar av administrativ respektive teknisk säkerhet, det vill säga samtliga behandlade delar i dessa riktlinjer.

I enlighet med vad som gäller för övrig verksamhet inom Högsby kommun, är ansvaret för informationssäkerheten kopplat till det delegerade verksamhetsansvaret. Det betyder att varje person som är ansvarig för en verksamhet eller får ett delegerat verksamhetsansvar också är ansvarig för informationssäkerheten i denna verksamhet.

## 1.5 Lagar och regler

Kraven på informationssäkerheten utgår från ledningens och verksamhetens krav på funktion och tillämplighet liksom legala krav, förordningar, föreskrifter, avtal och säkerhetskrav.

Verksamheten förväntas ha tillräcklig kunskap om de lagar och förordningar som gäller för respektive område.

Det finns myndigheter och organisationer som ger särskilt stöd genom att upprätta förteckningar om lagar och regelverk. Ett par av dessa listas nedan.

- Integritetsskyddsmyndigheten – https://www.imy.se
- MSB – Myndigheten för samhällsskydd och beredskap – Förteckning över lagar och regelverk som styr samhällets informationssäkerhet, https://www.informationssakerhet.se/lagar--regelverk/

## 1.6 Högsby kommuns övergripande styrdokument

*Informationssäkerhetspolicyn* beskriver Högsby kommuns syn på informationssäkerhet, viljeinriktning och stöd för informationssäkerhetsarbetet och de övergripande principer som gäller för informationssäkerheten. Informationssäkerhetspolicyn antas av kommunfullmäktige.

I policyn delegerar även kommunfullmäktige följande:

- vad och varför något skall åstadkommas
- vem som ansvarar för att detta uppnås
- hur detta skall följas upp

*Riktlinjer för informationssäkerhet* konkretiserar informationssäkerhetspolicyn och ger riktlinjer avseende skyddsåtgärder och -nivåer. Riktlinjer för informationssäkerhet är underställd informationssäkerhetspolicyn och fastställs av kommunstyrelsen.

Riktlinjerna innehåller bl. a:

- beskrivningar av hur ansvar och mål upprätthålls
- beskrivning av organisationen för informationssäkerhetsarbetet

*Tillämpningsanvisningar och instruktioner för informationssäkerhet* innehåller preciseringar till Högsby kommuns policy och riktlinjer. Tillämpningsanvisningar och instruktioner antas av kommunchef, förvaltningschef eller VD, som med stöd av Informationssäkerhetsstrateg och tillsammans med förvaltningar och bolag även tar fram en övergripande handlingsplan för informationssäkerhet inom respektive förvaltning eller bolag.

### 1.6.1 Lokala styrdokument

Varje förvaltning och bolagsstyrelse ska, inom ramen för Högsby kommuns övergripande ledningssystem för informationssäkerhet, styra och leda sitt informationssäkerhetsarbete inom dess verksamhetsområde.

Styrdokumenten på lokal nivå består av lokala anvisningar och rutiner för informationssäkerhet. Dessa styrdokument innehåller preciseringar och tillägg till de övergripande styrdokumenten med utgångspunkt från den egna verksamhetens specifika behov och i enlighet med tillämpningsanvisningar och instruktioner.

Med utgångspunkt från anvisningarna och instruktionerna utarbetas, då behov föreligger, lokala instruktioner av respektive förvaltning och bolag. De beskriver detaljerat hur rutiner och skyddsåtgärder utformas och tillämpas för att informationssäkerheten ska kunna realiseras i verksamheten.

Verksamhetens ordinarie processer skall inkludera informationssäkerhet och Införandet ska konkretiseras i en handlingsplan för informationssäkerhet.


## 1.7 Revision och ständig förbättring

Riktlinjerna ska revideras vid större förändringar, dock minst en gång per mandatperiod.

# 2 Termer och definitioner

För användningen av dessa riktlinjer gäller följande termer och definitioner

**Autentisering**
Kontroll av uppgiven identitet.

**Behandling av personuppgifter**
Varje åtgärd eller serie av åtgärder som någon vidtar med personuppgifter, vare sig det görs på automatiserad väg eller inte.

**Behörighet**
Tilldelad åtkomsträttighet i IT-system.

**Hot**
Möjlig oönskad händelse med negativa konsekvenser för verksamheten.

**Information**
Ett vitt begrepp som inkluderar allt från kunskap som enskilda medarbetare besitter till information lagrad i IT-system.

**Informationstillgång**
Med informationstillgång avses all information oavsett om den behandlas i ett IT-system, förekommer på ett utskrivet papper, i ett anteckningsblock, som ett samtal i korridoren eller i telefonen samt all form av film, ljud och bild.

**Informationsrisk**
Risk där konsekvensen uttrycks i konfidentialitet, riktighet, tillgänglighet eller spårbarhet

**Informationssäkerhet**
Bevarande av konfidentialitet, riktighet och tillgänglighet hos information. (Härutöver kan begreppet även innefatta till exempel spårbarhet, autenticitet, oavvislighet och tillförlitlighet).

**Informationssäkerhetsincident**
En eller flera händelser som kan tänkas få allvarliga konsekvenser för verksamheten och hota informationssäkerheten (till exempel brott mot sekretess, integritetsförlust, driftavbrott eller brist på tillgång till information).

**Informationssäkerhetspolicy**
Övergripande avsikt och viljeinriktning formellt uttryckt av en organisations ledning. Anger mål och inriktning för samt styr informationssäkerhetsarbetet inom organisationen.

**IT-system**
Informationsbehandlingssystem som med informationsteknik hanterar och utbyter information med omgivningen. I begreppet IT-system innefattas även kommunikationsutrustning, datorer, servrar, skrivare och övrig teknisk utrustning som ansluts till Högsby kommuns elektroniska kommunikationsnätverk.

**Konfidentialitet**
Egenskap att information inte görs tillgänglig eller avslöjas för obehöriga personer, enheter eller processer.

**Känsliga personuppgifter**
Uppgifter som avslöjar etniskt ursprung, politiska åsikter, religiös eller filosofisk övertygelse, medlemskap i fackförening samt uppgifter som rör hälsa eller sexualliv. Patientuppgifter är känsliga personuppgifter.

**Mobil enhet**
Mobiltelefon, surf- eller läsplatta eller liknande teknisk enhet. Bärbar dator innefattas inte i begreppet.

**Personuppgifter**
All slags information som direkt eller indirekt kan knytas till en fysisk person som är i livet. Bild- och ljuduppgifter om en identifierbar

fysisk person räknas som personuppgifter, även om inga namn nämns. Krypterade uppgifter och olika slag av elektroniska identiteter är också personuppgifter om de direkt eller indirekt kan kopplas till fysiska personer som är i livet.

**Riktighet**
Skydd mot oönskad förändring.

**Risk**
Produkten av sannolikheten och konsekvensen för att ett givet hot realiseras.

**Riskanalys**
Metodisk aktivitet som identifierar, beskriver och kvantifierar risk inom ett givet område, t ex ett system.

**Sammanhållen journalföring**
Ett elektroniskt system, som gör det möjligt för en vårdgivare att ge eller få direktåtkomst till personuppgifter.

**Samtycke**
Varje slag av otvetydig viljeyttring genom vilken den registrerade godtar att personuppgifter som rör honom eller henne behandlas.

**SCADA**
Supervisory Control and Data Acquisition, så kallade digitala kontrollsystem. Datorbaserade system för styrning, reglering och övervakning av fysiska processer som till exempel el-, gas- och vattenförsörjning samt spårbunden trafik.

**SITHS-kort**
Tjänstekort med elektronisk ID som används för autentisering vid inloggning till IT-system, främst vårdrelaterade.

**Skadlig kod**
Otillåten programkod som syftar till för att ändra, röja, förstöra, störa eller avlyssna ett datanät, funktioner eller uppgifter i IT-system.

**Skyddsåtgärd**
Handling, procedur eller tekniskt arrangemang som genom att minska sårbarheten möter identifierade hot.

**Spårbarhet**
Entydig härledning av utförda aktiviteter till en identifierad användare eller process.

**Stark autentisering**
Autentisering som innebär att identiteten kontrolleras på minst två sätt.

**Sårbarhet**
Brist i skyddet av en tillgång eller en grupp av tillgångar exponerad för hot.

**Tillgång**
Något som har värde för en organisation. Med informationstillgångar menas informationen i sig och de resurser som används för att hantera den, till exempel programvaror, tjänster och fysiska tillgångar.

**Tillgänglighet**
Egenskap att vara tillgänglig och användbar på begäran av en behörig aktör.

# 3 Riskbedömning och riskhantering

Varje verksamhet ska, för sin verksamhet, IT-system, processer och motsvarande, genomföra och dokumentera analyser avseende vilka hot, risker och sårbarheter som kan påverka verksamheten, och utifrån dessa analyser vidta lämpliga säkerhetsskyddsåtgärder.

Riskbedömning ska, om inte särskilda skäl föreligger, ske med delprocesserna riskidentifiering, riskanalys, riskvärdering och genomföras i enlighet med Högsby kommuns gällande vägledning.

För varje risk som identifieras under riskbedömning ska ett riskhanteringsbeslut fattas. Riskhanteringsbeslut som innebär att risk inte kan godtas ska leda till åtgärdsplan för att minska risken till godtagbar nivå.

Riskbedömning och riskhantering ska vara en kontinuerlig process och stödja informationssäkerhetsarbetet. Riskbedömningar ska revideras när förutsättningar väsentligen förändras.

# 4 Organisation

Kommunens har en upprättad organisation med utpekade roller[1] och ansvar för informationssäkerheten. Ansvaret sträcker sig från den politiska ledningen, genom tjänstemannaledningen ner till varje enskild användare.

## 4.1 Roller och ansvar inom den politiska ledningen

Den politiska ledningen har det övergripande ansvaret för informationssäkerhet. Kommunfullmäktige, kommunstyrelsen och respektive facknämnders ansvar för informationssäkerhetsarbetet beskrivs kortfattat nedan.

### 4.1.1 Kommunfullmäktige

Kommunfullmäktige fastställer en policy för informationssäkerhet, vilken uttrycker viljeinriktningen för kommunens arbete med informationssäkerhet.

### 4.1.2 Kommunstyrelsen

Kommunstyrelsen fastställer riktlinjer för informationssäkerhet och har det yttersta ansvaret för kommunens informationssäkerhetsarbete samt kommunstyrelsens verksamheter. Kommunstyrelsen utser Dataskyddsombud och är ytterst personuppgiftsansvarig för sina verksamheter.

### 4.1.3 Utskott och nämnder

De kommunala utskotten och nämnderna har ansvaret för informationssäkerhetsarbetet inom sina respektive verksamheter/myndigheter. Myndighets- och Valnämnden är ytterst personuppgiftsansvariga för sina verksamheter.

[1] Förtydligande av vissa specifika och för informationssäkerhetsarbetet viktig roller framgår av ”Rollbeskrivningar inom informationssäkerhet och -förvaltning – Högsby kommun 2022”

## 4.2 Roller och ansvar i verksamheten

### 4.2.1 Kommunchef

Ansvarar att tillse att kvalitets- och informationssäkerhetsarbetet bedrivs så effektivt som möjligt, genom att visa ett tydligt stöd och fördela resurser.

### 4.2.2 Varje chef

Varje chef ansvarar för att det finns rutiner som säkerställer att underställda kan efterleva kommunens regelverk för informationssäkerhet.

### 4.2.3 Informationssäkerhetsstrateg

Har det övergripande och strategiska ansvaret att leda, utveckla och samordna informationssäkerhetsarbetet samt föreskriva de metoder som skall användas för riskanalys och informationsklassning.

### 4.2.4 Informationsägare

Den som äger och ansvarar för att informationen är riktig, tillförlitlig och hanteras enligt kommunens policy, riktlinjer och instruktioner, samt att all relevant lagstiftning följs och för det sätt på vilket informationen sprids. Informationsägaren är därmed riskägare för den information som ska hanteras i IT-systemet/lösningen.

De interna relationerna mellan informationsägare och systemägare ska, när det gäller informationssäkerhet, utgå från informationsägaren.

Informationsägare ska vara förvaltningschef/verksamhetschef.

Informationsägaren utser informationsförvaltare.

### 4.2.5 Systemägare

Den som äger och har det övergripande ansvaret för ett eller flera IT-system/tjänster/komponenter. IT-systemet/tjänsten/komponenten hanterar alltid en eller flera informationsmängd(er).

Systemägare ska vara förvaltningschef/verksamhetschef.

Systemägaren utser systemförvaltare.

### 4.2.6 Dataskyddsombud

Dataskyddsombud enligt Dataskyddsförordningen. Kommunen har skyldighet att tillsätta ett dataskyddsombud med sakkunskap om lagstiftning och praxis om dataskydd. Rollen skall vara självständig, rådgivande och övervakande i att kommunen följer reglerna i Dataskyddsförordningen.

### 4.2.7 Dataskyddssamordnare

Övervakar att organisationen följer dataskyddsförordningen, kontrollerar att organisationen följer interna styrdokument och fungerar som ett stöd till verksamheterna i deras arbete med dataskydd.

## 4.3 Övriga roller

Kommunens verksamhetsledning bestående av ledande tjänstemän har det organisatoriska ansvaret för arbetet med informationssäkerhet. Kommundirektören och förvaltningscheferna har särskilt ansvar för organisation, ledning och styrning av informationssäkerhetsarbetet.

Nedanstående roller beskrivs kortfattat, en detaljerad rollbeskrivning av utvalda roller återfinns i kommunens systemförvaltningsmodell.

### 4.3.1 Förvaltningschef

Förvaltningschef har på kommunchefens och utskottet/nämndens uppdrag att tillse att informationssäkerhetsarbetet bedrivs så effektivt som möjligt genom att visa ett tydligt stöd och tilldela resurser. Förvaltningschefen har ofta rollen som informationsägare och systemägare för förvaltningens system, men kan delegera detta ansvar till en verksamhetschef som då också utser informations- och systemförvaltare för respektive system (ansvaret att utse informationsförvaltare följer rollen informationsägare och likaså följer ansvaret att utse systemförvaltare rollen systemägare).

Anvisningar, rutiner och instruktioner avseende informationssäkerhet och -förvaltning för respektive förvaltning fastställs av förvaltningschef eller efter delegation av verksamhetschef, i vilket fall anvisningarna, rutinerna och instruktionerna då avser informationssäkerhet och -förvaltning i den specifika verksamheten.

### 4.3.2 Chefen för kommunala bolag och förbund

De kommunala bolagscheferna har på styrelsens uppdrag att tillse att informationssäkerhetsarbetet i bolaget bedrivs i enlighet med Högsby kommuns Informationssäkerhetspolicy och Riktlinjer för informationssäkerhet.

### 4.3.3 Informationsförvaltare

Den som aktivt förvaltar informationen på informationsägarens uppdrag. Syftet med informationsförvaltning är inte bara att bevara handlingarna och göra dem läsbara under den tid som krävs. Syftet är bättre uttryckt att bevara handlingar som bevis för transaktioner så länge dessa bevis krävs eller är av värde.

Informationsförvaltare ska finnas inom varje verksamhet i varje förvaltning på Högsby kommun.

### 4.3.4 Systemförvaltare

Den som aktivt förvaltar IT-systemet/tjänsten/komponenten på systemägarens uppdrag, ansvarar för den dagliga användningen av systemet och tillser att systemets funktionalitet samt planerade och beslutade aktiviteter genomförs och upprätthålls.

### 4.3.5 IT-strateg

Den som samordnar IT-säkerheten för kommunens IT-infrastruktur (t.ex. nät, servrar och annan hårdvara), i såväl intern som extern IT-infrastruktur.

## 4.4 Roller och ansvar gällande samordning och uppföljning

För att samordning och uppföljning av informationssäkerhetsarbetet ska kunna bedrivas effektivt ska det finnas ett informationssäkerhetsråd. Utöver informationssäkerhetsstrategen ska rådet bestå av informationssäkerhetsrepresentanter från respektive förvaltning och bolag. Rådets uppgift är att främja, stödja, samordna och följa upp Högsby kommuns informationssäkerhetsarbete på en övergripande nivå. Rådet ska främja erfarenhets- och kunskapsutbyte, bevaka vilket behov av stöd som finns i verksamheterna och föreslå förbättringar, förankra och samordna viktiga informationssäkerhetsaktiviteter samt följa upp efterlevnaden av Högsby kommuns riktlinjer för informationssäkerhet

# 5 Personalresurser och informationssäkerhet

Alla som arbetar i Högsby kommuns verksamheter måste förstå sitt ansvar för och bidra till att hantera och skydda kommunens informationstillgångar.

Detta kapitel beskriver vad som ska omfattas och beaktas i samband med rekrytering, anställning och avslutande av anställning avseende informationssäkerhet. Kommunens rutin för rekrytering och anställning finns beskriven på kommunens intranät.

## 5.1 Före anställning

Säkerställ att alla anställda och andra berörda förstår sitt ansvar och är lämpliga för de roller som de är tilltänkta för. Exempel på andra berörda roller är elever, politiker, inhyrd personal, tjänsteköp och leverantörer.

### 5.1.1 Bakgrundskontroll

Bakgrundskontroll på alla sökande för anställning ska utföras i enlighet med relevanta författningar, etiska krav och i proportion till verksamhetskraven, klassificeringen av information som de ges behörighet till och de upplevda riskerna. Den arbetssökandes formella meriter (såsom utbildning, yrkeslegitimation, referenser etc.) ska kontrolleras och den arbetssökandes identitet ska verifieras. Vid rekrytering till särskilt informationssäkerhetskritiska arbetsuppgifter bör ytterligare registerkontroller genomföras av de arbetssökande. Exempel på bakgrundskontroll är utdrag ur belastningsregistret för till exempel förskollärare.

Person som deltar i verksamhet eller anställs på befattning som har betydelse för rikets säkerhet ska säkerhetsprövas. För person som deltar i sysslor som är säkerhetsstrategiskt viktiga för Högsby kommun gäller samma förhållande.

*Kommentar:* Säkerhetsskyddslag (1996:627) och Säkerhetsskyddsförordning (1996:633) innehåller bestämmelserna om säkerhetsprövning.

### 5.1.2 Arbetsbeskrivning och anställningsvillkor

Verksamheterna ska i anställnings- eller arbetsvillkor inkludera ett uttalande om den anställdes ansvar för informationssäkerhet.

Informationssäkerhetsroller och ansvar ska finnas beskrivna i relevanta arbetsbeskrivningar. Särskild uppmärksamhet ska läggas på roller och ansvar för tillfälliga eller korttidsanställningar av personal som vikarier, studenter, praktikanter etcetera. Anställda ska göras medvetna om dessa ansvarsbeskrivningar.

Samtliga medarbetare ska göras medvetna om sina skyldigheter enligt anställningsavtal eller andra tillämpliga avtal samt om gällande regler för informationssäkerhet och tillämpliga lagkrav, t ex offentlighets- och sekretesslagen (2009:400).

Det ska vara tydligt vilken information som ägs av kommunen och att den inte får förstöras eller kopieras vid avslutande av anställning eller uppdrag.

## 5.2 Under anställning

Det är viktigt att säkerställa att anställda och andra berörda är medvetna om och uppfyller sitt ansvar för informationssäkerhet.

### 5.2.1 Ledningens ansvar

Varje chef ansvarar för att det finns rutiner som säkerställer att underställda kan efterleva kommunens regelverk för informationssäkerhet.

### 5.2.2 Disciplinära åtgärder

Anställda ska göras medvetna om att bristande efterlevnad av gällande regler för informationssäkerhet och sekretess kan vara misskötsel, vilket är ett brott mot anställningsavtalet. Motsvarande ska i förekommande fall gälla uppdragstagare som inte är anställda. Det ska finnas en formell och kommunicerad disciplinär process för att vidta åtgärder mot anställda som har brutit mot gällande informationssäkerhetsregler.

### 5.2.3 Sekretess

Inom den offentliga sektorn är sekretess för de anställda reglerat i lag. En sekretessförbindelse är därför inte möjlig att använda, utan ersätts av sekretesserinran. Denna skrivs inte under utan, som namnet säger, erinrar om gällande lagstiftning.

Sekretessen omfattar inte enbart den som är anställd av Högsby kommuns eller dess bolag. Vid anlitande av konsult eller annan extern uppdragstagare ska det klargöras om han eller hon deltar i verksamheten på samma sätt som en anställd.

Deltar personen inte i verksamheten på sådant sätt att offentlighets- och sekretesslagen blir tillämplig, ska tystnadsplikten regleras civilrättsligt, det vill säga i avtal.

### 5.2.4 Medvetenhet, utbildning och fortbildning i informationssäkerhet

Kommunens målsättning är att en god säkerhetskultur ska genomsyra kommunen. Med detta menas inte bara att medarbetarna har god kunskap om vilka säkerhetsregler som gäller utan att de också använder gott omdöme och kritiskt ifrågasätter händelser som kan påverka säkerheten.

Samtliga anställda inom kommunen ska få den utbildning i informationssäkerhet som krävs för att de ska kunna utföra sina arbetsuppgifter och för att säkerställa målen för informationssäkerheten. Utbildningens omfattning ska vara anpassad till det ansvar och de befogenheter som gäller för befattningen. Detsamma gäller även vid omplacering av redan anställda och när tillfällig personal och externa konsulter anlitas.

Anställda ska ha genomgått minst en grundläggande utbildning inom informationssäkerhet som exempelvis DISA, Datorstödd informationssäkerhetsutbildning för användare.

Verksamheten ska föra en förteckning över vilka som har genomgått utbildning i informationssäkerhet. Utbildningsinsatserna bör följas upp årligen.

### 5.2.5 Mobila enheter

Alla mobila enheter (mobiltelefoner och surfplattor) som nyttjas för yrkesutövning inom Högsby kommuns beslutade verksamhetsområden (lagstadgade och av politiken fastställda) ska administreras via ett MDM-verktyg (Mobile Device Management) och vara registrerade hos Högsby kommun. Detta innebär också att inga privatägda mobila enheter bör användas inom ramen för de anställdas yrkesutövning.

Det ska finnas regler för hantering av mobila enheter som hanterar de risker som användning av mobila enheter medför. Vid användning av mobila enheter bör särskild försiktighet iakttas för att säkerställa att verksamhetsinformation inte äventyras.

Reglerna för mobila enheter ska hantera och beakta följande:

- Registrering av mobila enheter
- Krav på fysiskt skydd
- Begränsning av installation av program
- Krav på programversioner för mobila enheter och på att göra uppdateringar
- Begränsning av anslutning till informationstjänster
- Styrning av åtkomst
- Krypteringsteknik
- Skydd mot skadlig kod
- Avaktivering, radering eller låsning av konto på distans

- Säkerhetskopiering
- Användning av webbtjänster och webbtillämpningar

Utbildning bör ordnas för personal som använder mobila enheter för att öka deras medvetenhet om de ytterligare risker som följer av detta sätt att arbeta och vilka säkerhetsåtgärder som bör vara införda. T ex bör det finnas rutiner för användning av mobila enheter på offentliga platser, i mötesrum och på andra oskyddade områden, samt rutiner som beaktar fysiskt skydd för mobila enheter som lämnas obevakade då de kan innehålla viktig, känslig eller kritisk verksamhetsinformation.

#### *5.2.5.1 Användning av privata mobila enheter inom ramen för de anställdas yrkesutövning*

Användning av privata mobila enheter ska i så stor utsträckning som möjligt undvikas. I specifika fall kan det dock vara nödvändigt för att få en fungerande verksamhet. I dessa specifika fall ska reglerna för privata mobila enheter hantera följande:

- Separation av privat och yrkesmässig användning av enheter, inklusive användandet av program för att stödja sådan separation (se *5.2.5 Mobila enheter*) samt skydda verksamhetsdata på en privat enhet;
- Endast ge tillgång till verksamhetsinformation efter det att användaren har tecknat ett avtal där slutanvändaren bekräftar sina skyldigheter (fysiskt skydd, uppdatering av programvara, etc.), avstår från ägandet av verksamhetsdata, tillåter radering av data på distans av organisationen i händelse av stöld eller förlust av enheten eller när användaren inte längre har rätt att använda tjänsten. Reglerna måste också ta hänsyn till lagstiftning gällande skydd av personuppgifter.

### 5.2.6 Distansarbete

Distansarbete avser alla former av arbete utanför kontoret inklusive icke-traditionella arbetsmiljöer. Regler och stödjande säkerhetsåtgärder bör införas för att skydda information som nås, bearbetas eller lagras på distansarbetsplatser.

## 5.3 Avslut eller ändring av anställning

Högsby kommuns intressen ska, som en del i processen, skyddas vid ändring eller avslut av en anställning.

### 5.3.1 Avslut eller ändring av anställds ansvar

Det ska finnas en rutin som hanterar när medarbetare (anställda, praktikanter och inhyrda konsulter) slutar sin anställning eller uppdrag inom kommunen. Rutinen ska säkerställ att ansvarsuppgifter ska avlämnas och åtkomsträttigheter upphöra vid anställningens eller uppdragets slut. Den ska även säkerställa att nycklar, tjänstekort och övrig utrustning återlämnas.

# 6 Hantering av tillgångar

I detta kapitel finns det konkreta riktlinjer för hur vi ska hantera våra informationstillgångar. Sekretessbelagda handlingar och brukaruppgifter är exempel på känslig information som vi måste hantera på särskilt sätt. Genom att placera informationstillgångar i särskilda säkerhetsklasser vet vi vilka som kräver mer skydd än andra.

Med tillgång avses här tillgångar som är relaterade till information och informationssystem.

## 6.1 Förteckning över informationstillgångar

Det ska finnas en förteckning över viktiga tillgångar inom respektive verksamhet. Förteckningen ska identifiera det tillgångar som är relevanta i livscykeln för information och dokumentera deras betydelse för organisationen. Livscykeln för information bör omfatta skapande, bearbetning lagring, överföring, radering, och förstörelse (gallring), se Högsby kommuns *Informationshanteringsplan*. Förteckningen ska omfatta all sådan information som är nödvändig för återhämtning efter en störning eller allvarlig incident. Förteckningen över informationstillgångar ska vara korrekt, uppdaterad, konsistent och överensstämma med övriga register.

För varje identifierad tillgång ska en ägare utses (*se 6.2 Ägarskap av tillgångar*) och en klassificering genomföras (*se 6.3 Klassificering av information*)

## 6.2 Ägarskap av tillgångar

Tillgångar som återfinns i förteckningen över informationstillgångar ska tilldelas en ägare.

Medarbetare såväl som andra organisationsenheter som har accepterat förvaltningsansvar för informationstillgångens livscykel har kvalificerat sig för att tilldelas ägarskap över informationstillgången.

Ägarskap ska tilldelas när informationstillgångar skapas eller överförs till Högsby kommun. Informationstillgångens ägare ska ansvar för en korrekt förvaltning av informationstillgången och dess livscykel.

Informationstillgångens ägare ska:

- Se till att informationstillgångarna är inventerade
- Säkerställa att informationstillgångarna på ett lämpligt sätt klassificerats och skyddas
- Definiera och periodvis granska åtkomstbegränsningar och klassificeringar avseende viktiga informationstillgångar med hänsyn tagen till regler för åtkomststyrning
- Säkerställa korrekt hantering när informationstillgången tas bort eller förstörs

Identifierad ägare kan vara antingen en person eller en enhet som har accepterat förvaltningsansvar för att styra hela informationstillgångens livscykel. Identifierade ägare har nödvändigtvis inte någon äganderätt till informationstillgången.

Rutinuppgifter kan delegeras till någon som ansvarar för översyn av informationstillgångar på daglig basis (*se 4.3.3 Informationsförvaltare*), men ansvaret ligger hos informationsägaren.

I komplexa informationssystem kan det vara bra att fastställa grupper av informationstillgångar som tillsammans tillhandahåller eller utgör en viss tjänst. I detta fall är ägaren av denna tjänst ansvarig för leverans av tjänsten, inklusive driften av dess informationstillgångar.

## 6.3 Klassificering av information

Information bör klassas i termer av rättsliga krav, värde, verksamhetsbetydelse och känslighet för obehörigt röjande eller modifiering.

Respektive informationstillgång ska tilldelas en informationssäkerhetsklass som motsvarar dess betydelse för den aktuella verksamheten, se Högsby kommuns *Informationshanteringsplan*. Även system och andra resurser bör klassificeras om de till exempel är starkt knutna till viss information.

Ägaren av respektive informationstillgång ska ansvara för informationstillgångens klassning.

Vid informationsklassificering ska Högsby kommuns gällande klassificeringsmodell användas, se anvisning ”*Informationsklassningsmodell – Högsby kommun 2022”*.

Modellen för informationsklassificering ska baseras på säkerhetsaspekterna konfidentialitet, riktighet och tillgänglighet. Nivåbestämningen ska utgå från bedömd skada vid obehörig åtkomst, bristande riktighet och bristande tillgänglighet till informationstillgång.

Rutiner för klassificering ska fastställas i verksamhetens anvisningar.

Enligt *1.4 Grunder* ska alla viktiga informationstillgångar inom Högsby kommun klassificeras för att identifiera tillgångar som på ett eller annat sätt ställer högre krav på säkerhet. Klassificeringen av informationstillgångar ska ligga till grund för vilka skyddsåtgärder som ska utformas och vilka rutiner som ska gälla, det vill säga hur informationen får hanteras, lagras, distribueras och avvecklas. Strävan är att åstadkomma en konsistent bedömning av en och samma informations värde – oavsett var (eller av vilken verksamhet) informationen hanteras.

## 6.4 Hantering av tillgångar

Rutiner som överensstämmer med informationens klassning ska upprättas för hantering, bearbetning, lagring och kommunikation av information (*se 6.3 Klassificering av information*)

## 6.5 Hantering av sekretessbelagd information

En offentlig verksamhets informationshantering styrs av ett omfattande regelverk, däribland grundlagarna. De viktigaste för Högsby kommun är tryckfrihetsförordningen, offentlighets- och sekretesslagen, arkivlagen och förvaltningslagen.

Innan information lämnas till allmänheten ska en sekretessbedömning genomföras. Om någon osäkerhet finns ska juridisk sakkunnig kontaktas. Den person som lämnar ut informationen ska försäkra sig om att det är rätt person som får den.

Det ska finnas lokala instruktioner och rutiner för utlämnande av information. I dessa ska det framgå vem eller vilka som har rätt att fatta beslut om ett utlämnande.

*Kommentar:* Alla handlingar som skapas, kommer in till eller som ska skickas från en myndighet är i princip allmänna och normalt offentliga och ska vara tillgängliga för allmänheten. Det finns dock allmänna handlingar där uppgifter sekretessmarkerats eller hemligstämplats av olika skäl. Information och instruktioner om vilka krav som ställs på hantering av handlingar och arkivering finns i Högsby kommuns informationshanteringsplan som är beslutad av fullmäktige.

## 6.6 Bevarande, rensning och gallring av information

Allmänna handlingar som finns i offentlig verksamhet får enbart gallras enligt Högsby kommuns beslutade informationshanteringsplan. Detta gäller oavsett i vilket medium handlingen finns lagrad.

Handlingar som finns inom offentlig verksamhet och som inte är allmänna kan rensas vid behov, men bör stämmas av mot *Informationshanteringsplanen*. Varje handläggare är ansvarig för att avgöra vilka handlingar som kan rensas och vilka som är allmänna i enlighet med de regler som finns (*se Informationshanteringsplanen*) och oavsett i vilket medium handlingen finns lagrat.

*Kommentar*: Med gallring i offentlig verksamhet menas avsiktlig och kontrollerad förstöring av allmänna handlingar. Beslutanderätten om gallring är inom Högsby kommun reglerat i informationshanteringsplanen. Alla Högsby kommuns verksamheter ska ha en informationshanteringsplan.

## 6.7 Personuppgifter

I samband med insamling av personuppgifter ska den enskilde informeras om behandlingen och om sina rättigheter. Grundtanken är att personer ska kunna fatta välinformerade beslut innan de lämnar uppgifter till Högsby kommun. Det är informationsägarens eller ytterst den personuppgiftsansvariges ansvar att det finns instruktioner och rutiner inom området.

Behandling av personuppgifter, t ex i ett IT-system, måste anmälas och förtecknas hos den personuppgiftsansvarige (*se även 6.1 Förteckning över informationstillgångar*).

## 6.8 Skyddade personuppgifter

Alla personer, såväl medborgare, brukare som medarbetare, ska kunna känna sig trygga med att deras personuppgifter inte kommer i orätta händer. Informationsutbyte, elektronisk eller icke-elektronisk, får inte leda till att skyddade uppgifter röjs eller avslöjas.

Förvaltningar, bolag och stiftelser ska utforma anvisningar och rutiner för behandling av skyddade personuppgifter.

Personuppgifter som är skyddade ska vara tydligt märkta så att detta framgår för personer som hanterar dem.

Vid upphandling av IT-system ska hantering av skyddade personuppgifter beaktas särskilt. IT-system ska utformas så att så få personer som möjligt med särskild behörighet har tillgång till sådana uppgifter.

# 7 Användning av IT-system

Hur får anställda använda datorer, internetuppkoppling, telefoner, e-post och andra arbetsredskap för att vi ska ha god informationssäkerhet?

Här finns riktlinjerna för den personliga användningen av Högsby kommuns IT-system, och för vad som gäller vid arbete på annat ställe än arbetsplatsen.

## 7.1 Generella regler för användning av Högsby kommuns IT-system

Högsby kommuns IT-resurser (datorer, mobila enheter, nätverk och kringutrustning) är avsedda att användas som arbetsredskap vid tjänsteutövning. Privat användning av till exempel Officepaketet, internet och e-post är tillåten i sådan omfattning att det inte inkräktar på arbetet eller medför onödiga risker eller kostnader för Högsby kommun.

Högsby kommuns utrustning ska användas för arbetsrelaterade ändamål. Information ska så fort det är möjligt sparas på anvisad plats i nätverket.

För att förhindra obehörig åtkomst till IT-system ska användaren inte lämna PC-arbetsplats inloggad. När PC-arbetsplats lämnas ska den låsas (snabbkommando: Windows-knapp + L).

Vid förlust av IT-utrustning ska detta snarast anmälas till verksamhetens IT-avdelning enligt gällande rutin.

Om skadlig kod (till exempel datorvirus) upptäcks ska verksamhetens IT-avdelning omedelbart kontaktas enligt gällande rutin.

## 7.2 Anslutning av utrustning i Högsby kommuns IT-system

Användare får endast ansluta av Högsby kommun tillhandahållen och kontrollerad IT-utrustning till Högsby kommuns allmänna nätverk (hk.hogsby.se och till hk.hogsby.se anslutna LAN).

Anslutning av IT-utrustning som inte tillhandahållits och kontrollerats av Högsby kommun (som medtas av till exempel brukare, anhöriga och andra besökare) ska ske till Högsby kommuns publika nätverk (PubKommun och PubKommun5G) som är logiskt separerat från Högsby kommuns allmänna nätverk.

Anslutning av IT-utrustning som inte tillhandahållits av Högsby kommun men som krävs för att utföra arbete på uppdrag av verksamheten (som medtas av till exempel konsulter och leverantörer) ska regleras i skriftligt avtal, där det anges vilka säkerhetsåtgärder som ska vidtas för att skydda verksamhetens IT-miljö och informationstillgångar.

IT-utrustning som är ansluten till Högsby kommuns allmänna nätverk (hk.hogsby.se och till hk.hogsby.se anslutna LAN) får inte samtidigt vara uppkopplad mot annat nätverk utanför Högsby kommuns kontroll.

Anställdas anslutning till Högsby kommuns allmänna nätverk ska vid arbete från annan plats ske genom en kommunikationslösning som är godkänd av Högsby kommun (via ADFS-tjänsten, Always on VPN anslutning till hk.hogsby.se).

## 7.3 Användning av Högsby kommuns IT-system

Övergripande princip för all nätverksåtkomst via Högsby kommuns nätverk är att användare och IT-system endast ska ha tillgång till de IT-system de har behörighet till, det vill säga man ska via nätverks- och brandväggsregler nekas åtkomst till system man ej har explicit behörighet att använda.

Information som rör Högsby kommuns verksamhet ska som regel bearbetas och lagras med hjälp av IT-system som har tillhandahållits av Högsby kommun.

Vilken slags information som får bearbetas, lagras, eller kommuniceras i olika IT-system ska framgå av systemspecifika bestämmelser som ska grundas på av informationsägaren uttalade säkerhetskrav.

IT-systemens skyddsmekanismer och säkerhetsprogramvaror ska hållas uppdaterade och får inte kringgås eller sättas ur spel.

Endast behöriga ska få tillgång till verksamhetens IT-system. Användaren ska hantera IT-utrustning på ett sätt som minimerar risken för att obehöriga får tillgång till den, att den stjäls eller går förlorad.

Användare får endast installera programvaror eller IT-system som tillhandahålls eller godkänts av verksamheten i enlighet med verksamhetens anvisningar och instruktioner.

Användaren ska följa gällande lagstiftning, Högsby kommuns riktlinjer och värdegrund samt verksamhetens anvisningar och instruktioner.

Om IT-utrustning ska utrangeras, kasseras, säljas eller på annat sätt lämna verksamheten ska detta utföras i enlighet med av systemägarens utfärdade instruktioner.

När fasta eller löstagbara lagringsmedier som innehåller personuppgifter inte längre ska användas för sitt ändamål ska lagringsmedierna förstöras alternativt raderas på ett sådant sätt att uppgifterna inte kan återskapas.

### 7.3.1 Särskilda riktlinjer för mobila enheter

Samma hanteringsregler ska gälla för mobila enheter som till exempel mobiltelefoner och surfplattor som för övrig IT-utrustning. Konkretiserande regler för mobila enheter ska finnas i verksamhetens anvisningar och instruktioner.

### 7.3.2 Särskilda riktlinjer för lagring i extern lagringstjänst eller på externt lagringsmedium

Vid extern lagring av Högsby kommuns information som är klassad med förhöjda krav på tillgänglighet, riktighet eller konfidentialitet, ska det vara säkerställt att den externa lagringstjänsten eller det externa lagringsmediet kan uppfylla dem (*se 9.11 Drift hos extern part*).

Regler för användning av externa lagringstjänster ska finnas i verksamhetens anvisningar och instruktioner.

*Kommentar:* Ovanstående innebär bland annat att en användare som avser behandla känsliga personuppgifter i till exempel en molntjänst måste göra en bedömning om behandlingen är tillåten enligt dataskyddsförordningen och offentlighets- och sekretesslagen. Huvudregeln är att det inte är tillåtet att behandla känsliga personuppgifter i externa lagringstjänster om inte särskilda skyddsåtgärder vidtas. Kravet innebär även att användare måste iaktta särskild försiktighet vid användande av till exempel mobiltelefoners funktioner för lagringstjänster.

## 7.4 Privat användning av Högsby kommuns IT-system

Privat behandling av information med hjälp av Högsby kommuns IT-system måste alltid styras av måttfullhet och av den enskildes goda omdöme så att den inte stör Högsby kommuns verksamhet.

Regler för bisysslor ska finnas i verksamhetens anvisningar och instruktioner. Av dessa ska framgå att anställda inte får använda sig av arbetsgivarens egendom, till exempel IT-system, vid utövande av bisyssla och att bisyssla inte får leda till att skyddet av Högsby kommuns informationstillgångar åsidosätts.

*Kommentar:* Vid privat användning av Högsby kommuns IT-system ska användaren följa gällande lagstiftning, Högsby kommuns riktlinjer och värdegrund.

## 7.5 Användning av Internet

En användare ska inte använda Högsby kommuns IT-system på ett sådant sätt att det finns risk för att Högsby kommuns anseende skulle kunna skadas eller att användningen kränker någon annan person. Högsby kommuns anseende skulle till exempel kunna skadas om en användare besöker olagliga eller olämpliga webbsidor på Internet, eftersom det då är myndighetens IP-adress som exponeras.

Användaren ska agera säkerhetsmedvetet och inte besöka internetsidor som bedöms innebära säkerhetsrisker för Högsby kommuns IT-miljö, för att undvika exempelvis virusangrepp eller onödig belastning av Högsby kommuns nätverk.

Användaren ska vara medveten om att användande av Internet som sker via Högsby kommuns IT-system utifrån sett uppfattas som att det är Högsby kommuns som använder Internet.

Användaren ska vara medveten om att besök på webbplatser på Internet lämnar elektroniska spår efter sig. Med hjälp av så kallade cookies (det vill säga de textfiler som sparas i en dator som varit uppkopplad mot Internet) kan andra registrera vilka webbplatser Högsby kommuns medarbetare besöker.

## 7.6 Användning av e-post

Innehavaren av e-postlåda är ansvarig för vad som skickas eller lagras och ska säkerställa att myndighetspost hanteras på ett korrekt sätt. Användaren ska vara medveten om att e-post som skickas till eller från Högsby kommuns e-postadresser eller som finns i Högsby kommuns IT-system kan uppfattas som Högsby kommuns e-post.

Varje användare ska utan dröjsmål avgöra om den skickade eller mottagna e-posten utgör allmän handling. E-post som utgör allmän handling ska utan dröjsmål hanteras och registreras i enlighet med gällande regler. E-post som utgör allmän handling får ej heller vidarebefordras, utan då flera användare har behov av att ta del av informationen ska de istället informeras om var den allmänna handlingen finns att tillgå.

Användaren ska, som grundregel, betrakta e-post som oskyddad och Högsby kommuns nätverk som öppna (osäkra). Detta innebär att meddelanden som skickas okrypterade via e-post inte kan betraktas vara skyddade från insyn, och att det därmed finns risk för att andra än den avsedda mottagaren kan ta del av innehållet.

Information som omfattas av sekretess eller är klassad K3 eller högre enligt Högsby kommuns informationsklassningsmodell (se kapitel *6 Hantering av tillgångar*) ska skyddas med e-postkrypteringslösning som godkänts av verksamhetens IT-avdelning, t ex SecureMailbox, då den skickas internt eller externt i e-postsystemet. Informationen ska i sådana fall inte lagras i e-postsystemet längre tid än nödvändigt.

Sekretessbelagda eller integritetskänsliga personuppgifter som inkommit oskyddade via e-post ska utelämnas ur ett oskyddat e-postsvar eller vidarebefordran, så att de inte sprids vidare i öppna nätverk.

Det är vid tjänsteutövning endast tillåtet att använda e-postadressen förnamn.efternamn@hogsby.se eller annan av arbetsgivaren tilldelad arbetsplatsadress.

Personer som har en tjänst som innebär hantering av allmänna handlingar ska genom fullmakt delegera ansvaret för sin e-post under perioder som semester och frånvaro. Tjänsten ”Autosvar” ska aktiveras i Microsoft Outlook och det ska framgå vilken person som innehar det delegerade ansvaret under frånvaron.

Regler för e-post ska finnas i verksamhetens anvisningar och instruktioner. Av dessa ska framgå att information som skickas och tas emot med Högsby kommuns e-post eller är lagrad i Högsby kommuns e-postbrevlådor omfattas av tryckfrihetsförordningen samt offentlighets- och sekretesslagen, arkivlagen m.fl. på samma sätt som övriga handlingar.

Kommentar: Användaren ska vara medveten om att nämnder och styrelser inom Högsby kommun är egna förvaltningsmyndigheter. E-post som skickas inom Högsby kommuns egna nät från en förvaltningsmyndighet (expedierande myndighet) till en annan kan vara en allmän handling hos den mottagande förvaltningsmyndigheten. Mer information om hantering av sekretessbelagd information finns i avsnittet *6.5 Hantering av sekretessbelagd information*.

## 7.7 Användning av sociala medier

Ingen känslig information i strid med svensk lag eller Högsby kommuns riktlinjer eller värdegrund får kommuniceras i sociala medier.

Det är inte tillåtet att använda samma lösenord till sociala medier som till Högsby kommuns interna system. I övrigt gäller motsvarande regler som för e-post.

Registrering av Högsby kommuns e-postadress i sociala medier får endast ske om det ingår i Högsby kommuns verksamhet.

## 7.8 Användaridentiteter, lösenord och e-tjänstekort

Användaridentiteter, lösenord, e-tjänstekort (SITHS-kort) och mobila e-legitimationer (Freja eID+/Organisations ID) är personliga och får inte lånas ut.

Användare ansvarar för att användaruppgifter (till exempel lösenord) inte blir kända för andra. I de fall användaruppgifter blir kända för andra ansvarar användaren för att lösenordet utan dröjsmål byts i aktuellt IT-system.

Vid misstanke om att ett lösenord kommit i fel händer eller ett e-tjänstekort (SITHS-kort)/mobil e-legitimation (mobiltelefon) har tappats bort måste det omgående rapporteras så att de kan spärras och bytas ut.

## 7.9 Kontrollåtgärder

Information om vad som sker på en användares dator lagras i enskild dator, s.k. loggning. Loggning görs för driftövervakning och felsökning men kan även göras för uppföljning av att gällande regler och riktlinjer följs samt för att identifiera hot (t.ex. intrångsförsök och skadlig kod) som kan utgöra en fara för Högsby kommuns IT-miljö och/eller informationstillgångar.

Medarbetares användning av Högsby kommuns IT-system kan komma att följas upp vid misstanke om brott mot lag eller Högsby kommuns styrande regelverk.

Kommunchef, förvaltningschef eller motsvarande, eller person med delegation därifrån, beslutar om kontroll av medarbetares användning ska ske och om några åtgärder ska vidtas i det enskilda fallet i samband med överträdelser. Kommunchef/Förvaltningschef/VD ska fastställa instruktioner för hur sådan kontroll ska genomföras.

Kommunchef/Förvaltningschef/VD eller motsvarande, eller person med delegation därifrån, beslutar om kontroll ska ske av trafiken i lokala nätverk. Kommunchef/Förvaltningschef/VD ska fastställa instruktioner för hur sådan kontroll ska genomföras.

Kommunchef, eller den som kommunchefen utser, beslutar om kontroll ska ske av loggar i central IT-infrastruktur i syfte att identifiera och oskadliggöra hot mot Högsby kommuns IT-miljö eller informationstillgångar. Kommunchefen, eller den som kommunchefen utser, fastställer instruktioner för hur sådan kontroll ska genomföras. Högsby kommuns förvaltningar och bolag och andra som genom avtal är bundna av dessa riktlinjer är skyldiga att bistå i detta arbete.

Medarbetares tillgång till Högsby kommuns IT-system kan stängas av vid misstanke om brott mot lag eller Högsby kommuns styrande regelverk eller då användningen utgör en allvarlig risk för Högsby kommuns IT-miljö och/eller informationstillgångar.

Anslutning till hk.hogsby.se kan komma att stängas av då anslutningen utgör hot mot Högsby kommuns IT-miljö och/eller informationstillgångar. Beslut om sådan avstängning ska fattas av systemägaren för hk.hogsby.se, eller person med delegation därifrån. Innan beslut om avstängning fattas ska riskerna med avstängningen ha analyserats.

# 8 Åtkomst till information

Hur vi ska förhindra att obehöriga får åtkomst till Högsby kommuns informationssystem, IT-tjänster och - infrastruktur? Här finns riktlinjer för hur åtkomsten till informationen administreras, kontrolleras och loggas så att endast behöriga användare kommer åt information.

Åtkomst till information ska regleras av ägaren till informationstillgången. Ägaren ska fastställa lämpliga regler för styrning av åtkomst, rättigheter och begränsningar för specifika roller. Detaljrikedom och hur stränga säkerhetsåtgärderna är bör avspegla de säkerhetsrisker som är förknippade med informationen.

## 8.1 Styrning av åtkomst till elektronisk information

All tillgång till elektronisk information inom Högsby kommuns ska styras med hjälp av administrativa och tekniska skyddsåtgärder: åtkomstadministration, åtkomstkontroll samt loggning och uppföljning, så att endast behöriga får tillgång till IT-system och informationen i dem.

Den som är inloggad i ett IT-system ansvarar för vem som tar del av informationen. Om flera organisationer är ägare till information i ett och samma system ska avtal skrivas om gemensamma rutiner.

Det ska finnas en funktion som säkerställer automatisk utloggning ur IT-system eller aktivering av lösenordskyddad skärmsläckare efter en viss tids inaktivitet.

### 8.1.1 Särskilda riktlinjer för åtkomstadministration - åtkomsträttigheter

Åtkomsträttigheten ska godkännas av informationsägare eller motsvarande innan den delas ut. Rättigheterna ska vid varje tillfälle baseras på användarens aktuella behörighet, utifrån arbetsuppgifter och organisatorisk tillhörighet och fastställa användarens åtkomsträttigheter. Åtkomsträttigheterna styr vilka data som kan nås av en viss användare och vad användaren kan göra med data, t ex läsa, skriva, radera och exekvera.

Rutiner ska fastställas för hur beställning, registrering, ändring och avregistrering av rättigheter ska göras.

Innan en användare tilldelas åtkomsträttighet ska en behovs- och riskbedömning göras. Användaren ska ha tillräckliga kunskaper och utbildning i informationssäkerhet.

Tilldelning av åtkomsträttigheter ska dokumenteras och regelbundet följas upp. Detta ska även ske efter varje större organisations- eller systemförändring.

Åtkomst med utvidgade rättigheter, så kallade administratörsrättigheter, ska begränsas till så få personer som möjligt och baseras på deras behov av åtkomst anpassat till situationen och minimikravet för deras funktionella roll.

Beslut om nya administratörsrättigheter ska vara skriftliga och fattas av informationsägaren, varför nya administratörsrättigheter inte tilldelas förrän godkännandeprocessen är klar.

Administratörsrättigheter ska tilldelas användarkonton som är särskilda från de konton som används för ordinarie verksamhet. Ordinarie aktiviteter ska ej heller utföras från användarkonton med administratörsrättigheter.

Systemadministrativa arbetsuppgifter ska alltid vara kopplade till personliga användaridentiteter, för att säkerställa spårbarhet avseende genomförda aktiviteter.

### 8.1.2 Särskilda riktlinjer för åtkomstadministration – borttagning eller justering av åtkomsträttigheter

Åtkomsträttigheter för alla anställda, och externa användare, till information och informationsbehandlingsresurser ska tas bort vid avslutande av deras anställning, avtal eller uppdrag och justeras vid förändringar.

När en anställning avslutas ska individens åtkomsträttigheter till information och tillgångar som är kopplade till informationsbehandlingsresurser och -tjänster avlägsnas eller avslutas. Förändringar i anställningen ska återspeglas i avlägsnandet av alla rättigheter som ej längre är godkända för den nya rollen. Rättigheter som ska tas bort eller justeras omfattar fysisk och logisk åtkomst. Dokumenterad information som identifierar åtkomsträttigheter för anställda och entreprenörer ska återspegla avlägsnad eller justerad nyttjanderätt. Om en avgående medarbetares eller en extern parts användarkonto är aktivt ska lösenordet ändras vid uppsägning eller vid förändring av anställning, avtal eller överenskommelse.

Åtkomsträttigheter för information och tillgångar som är kopplade till informationsbehandlingsresurser ska reduceras eller tas bort innan anställningen upphör eller ändras, beroende på utvärdering av riskfaktorer såsom:

- Om avslutande eller ändring av anställning är initierad av den anställde, den externa parten eller av ledningen och orsaken till den avslutande anställningen;
- Medarbetarens, den externa partens eller annan användares nuvarande ansvar;
- Värdet av de tillgängliga tillgångarna.

Under vissa omständigheter kan åtkomsträttigheter vara fördelade på flera personer, t ex genom delade användarkonton. När en person slutar ska i dessa fall personen ifråga tas bort från gruppåtkomstlistor och åtgärder ska vidtas för att informera övriga anställda och externa parter om att de inte längre ska dela denna information med den person som slutar.

### 8.1.3 Särskilda riktlinjer för åtkomstkontroll - identitet

Varje användares identitet ska verifieras. Detta sker genom autentisering, det vill säga verifiering av användarens identitet. Alla användare ska ha en unik identitet. Det grundläggande kravet på utformningen av identiteter är att de ska vara spårbara till en fysisk person.

Användare bör vara skyldiga att underteckna en försäkran om att hålla konfidentiell personlig autentiseringsinformation konfidentiell och att hålla gruppens (vid delade användarkonton) hemliga autentiseringsinformation enbart inom gruppen. Denna skriftliga försäkran ska ingå i anställningsvillkoren, se *5.1.2 Arbetsbeskrivning och anställningsvillkor*.

Det ska finnas rutiner för säkerställande av identiteten på en användare innan konfidentiell autentiseringsinformation tilldelas, oavsett om informationen är ny, förnyad eller tillfällig.

Tillfällig konfidentiell autentiseringsinformation ska ges till användare på ett säkert sätt och användning av externa parter eller oskyddade (klartext) elektroniska meddelande ska undvikas. Tillfällig konfidentiell autentiseringsinformation ska också vara unik för en individ och ska inte heller gå att gissa sig till.

E-legitimation via kort eller mobil e-legitimation med PIN-kod (tillitsnivå 3) ska användas för att säkerställa att användare av IT-system är behöriga. Vid information i lägre skyddsklasser och när det inte är möjligt att använda e-tjänstekort eller mobil e-legitimation (tillitsnivå 3), ska användaridentitet i kombination med lösenord och SMS-kod (tillitsnivå 2) eller användaridentitet i kombination med lösenord användas (tillitsnivå 1).

#### *8.1.3.1 Lösenordshantering*

System som hanterar lösenord bör:

- Tvinga användning av individuella användarkonton och lösenord så att individuellt ansvar kan utkrävas;
- Låta användare själva välja och ändra sina lösenord och innehålla en rutin som ger; meddelande om inmatningsfel;
- Säkerställa att lösenord av hög kvalitet väljs, d v s lösenord som:
    - Inte är baserade på något en annan person lätt kan gissa eller få fram med personrelaterad information, t ex telefonnummer och födelsedatum;
    - Står emot ordlisteattacker (d v s inte består av ord i ordböcker);
    - Inte består av identiska enbart numeriska eller enbart alfabetiska tecken;
- Tvinga användarna att ändra sina lösenord vid första inloggningen;
- Kräva ändring av lösenord regelbundet samt vid behov;
- Upprätthålla ett register över tidigare använda lösenord och förhindra användning av tidigare använda lösenord;
- Inte visa lösenord på skärmen vid inmatning;
- Lagra lösenordsfiler åtskilt från data för tillämpningssystem;
- Lagra och överföra lösenorden på ett säkert sätt.

### 8.1.4 Särskilda riktlinjer för loggning och uppföljning

Åtkomst ska loggas och tilldelade rättigheter följas upp för att säkerställa att endast behöriga användare har åtkomst till viss information.

Användarnas rättigheter ska ses över med jämna mellanrum, t ex halvårsvis och efter ändringar såsom vid befordran eller avslutad anställning. Administratörsrättigheter ska ses över oftare, t ex kvartalsvis. En användares rättigheter ska också ses över när användaren byter från en roll till en annan inom Högsby kommun.

Loggarna ska vara skyddade mot obehörig åtkomst och manipulation. Loggarna ska omfattas av fastställda rutiner för säkerhetskopiering och arkivering. För att säkerställa logginformationens värde, ska rutiner fastställas för synkronisering av loggade IT-systems systemklockor.

Systematiska och regelbundna stickprovskontroller ska göras av loggarna enligt fastställd rutin. Av denna ska framgå vad som ska loggas, hur ofta loggarna ska granskas, vem som ska utföra granskningen samt vad som är att betrakta som överträdelse. Vidare ska det finnas regler för hur överträdelser hanteras.

Användarkonton med administratörsrättigheter ska granskas regelbundet samt vid varje enskild förändring av sådant konto.

För system som har känslig information i informationsklassen K3 eller högre enligt Högsby kommuns informationsklassningsmodell, ska loggarna analyseras med hjälp av automatiserade verktyg med koppling till larm för när gränsvärden överskrids. Om detta inte är möjligt ska manuella kontroller göras vilka är så omfattande att alla medarbetare någon gång per år blir granskade. Extra vikt ska läggas vid uppföljning av administratörskonton.

Informationsägaren ska besluta om vilket säkerhetsskydd som är erforderligt gällande säkerhetskopierade loggar.

Vid hantering av information i K3 eller högre enligt Högsby kommuns informationsklassningsmodell ska loggarna sparas i tio år.

*Kommentar:* Det är informationsägarens ansvar att loggning sker på samtliga verksamhetskritiska IT-system, så att det i efterhand går att följa enskilda användares aktiviteter.

#### *8.1.4.1 Skydd av logginformation*

Det ska finnas säkerhetsåtgärder som syftar till att skydda mot obehöriga ändringar i logginformation och operativa problem med loggningsverktyg inklusive:

- Ändringar av de meddelandetyper som registreras;
- Loggfiler som redigeras eller tas bort;
- Kapaciteten för lagring av loggdata överskrids, vilket resulterar i antingen att registreringen av händelser upphör eller att tidigare registrerade händelser skrivs över.

#### *8.1.4.2 Administratörs- och operatörsloggar*

Då användare med administratörsrättigheter eventuellt kan manipulera loggar på informationsbehandlingsresurser är det nödvändigt att skydda och granska loggarna för att säkerställa ansvarsskyldighet för administratörer.

Ett intrångsdetekteringssystem utan åtkomsträtt från system- och nätverksadministratörer kan användas för att övervaka efterlevnad i system och nätverk.

#### *8.1.4.3 Synkronisering av tid*

Systemklockorna i alla relevanta informationsbehandlingssystem inom Högsby kommun bör synkroniseras mot en och samma referenskälla för tid, varför Högsby kommun bör implementera och dokumentera en tillförlitlig teknisk lösning för att tidssynkronisera interna klockor mot en extern referenstid.

Korrekt inställning av tid är viktig för att säkerställa riktigheten av granskningsloggar, som kan krävas för undersökningar eller som bevis i rättsliga eller disciplinära ärenden. Felaktiga granskningsloggar kan försvåra utredningar och skada trovärdigheten i bevis. En klocka som länkas till en tid från ett nationellt atomur kan användas som tid för loggsystemet. Ett protokoll för nätverkstid kan användas för att tidssynkronisera alla servrar.

## 8.2 Extern informationsanvändning

För informationsanvändare som ges åtkomst till Högsby kommuns icke-publika informationstillgångar från miljöer utanför Högsby kommuns kontroll, ska särskilda krav ställas på autentisering av användare och utrustning, liksom på kryptering. Formella regler, rutiner och säkerhetsåtgärder bör tas fram för att skydda överföring av information genom alla typer av kommunikationsmedel.

Säker överföring av verksamhetsinformation mellan Högsby kommun och externa parter ska vara reglerad i överenskommelser. En sådan överenskommelse (t ex ett PUB-avtal) bör innehålla följande:

- Ledningsansvar för att styra och anmäla överföring, sändning och mottagande
- Rutiner för att säkerställa spårbarhet och oavvislighet
- Tekniska minimistandarder för paketering och överföring
- Depositionsavtal
- Rutiner för identifiering av bud
- Ansvarsförhållanden och skadeståndsskyldighet i händelse av informationssäkerhetsincident, såsom förlust av data
- Användning av överenskommen märkning för känslig eller kritisk information, som säkerställer att innebörden av märkningen förstås omedelbart och att informationen skyddas på lämpligt sätt
- Tekniska standarder för registrering och att läsa information och program
- Särskilda säkerhetsåtgärder som krävs för att skydda känsliga tillgångar och objekt, t ex kryptering
- Att upprätthålla en ansvarskedja för information under överföring
- Acceptabla nivåer av åtkomststyrning

Rutiner för identifiering av och skydd mot skadlig kod som kan överföras vid elektronisk kommunikation ska tas fram, se även *10.5 Skydd mot skadlig kod*.

Vid tillgång till brukaruppgifter eller andra uppgifter i klassen K3 eller högre enligt Högsby kommuns informationsklassningsmodell ska de alltid krypteras med relevant metod och endast vara tillgängliga genom stark autentisering.

## 8.3 Styrning av åtkomst till icke digital information

Skriftlig information ska omgärdas av skyddsåtgärder vid all hantering, det vill säga kopiering, distribution, förändring, läsning, makulering, förvaring och arkivering. Rutiner ska finnas för detta.

När information förvaras i säkra utrymmen, för att den är högt klassificerad enligt Högsby kommuns informationsklassningsmodell, det vill säga K3 eller högre, ska en förteckning föras över de personer som har åtkomsträttigheter till det säkra utrymmet.

Ljud- och videoupptagningar ska hanteras i enlighet med gällande författningar. Lämpliga skyddsåtgärder ska införas som förhindrar obehörig åtkomst, manipulation eller oavsiktlig förstöring.

Utformningen av skyddsåtgärder när information byter bärare, till exempel när elektronisk information skrivs ut på papper eller förmedlas via telefon, måste anpassas. När information överförs muntligt bör den som förmedlar informationen förvissa sig om att mottagaren är den avsedda och att lämpliga skyddsåtgärder vidtagits mot att fel personer kan höra eller avlyssna. Innan information överlämnas ska mottagaren informeras om hur informationen ska hanteras och förvaras.

*Kommentar:* Ovanstående innebär till exempel att telefonsamtal med känslig information ska ske där det inte kan avlyssnas, att man inte lämnar meddelanden som innehåller känslig eller konfidentiell information på telefonsvarare eftersom dessa kan spelas upp av obehöriga, lagras på gemensamma system eller lagras felaktigt till följd av felslagning av nummer och att känslig information på presentationstekniska hjälpmedel som whiteboard ska skyddas och avlägsnas efter möte.

# 9 Kryptering

Kryptering är att göra information svårläslig för alla som inte ska kunna läsa den. Genom att kryptera vår kommunikation och våra filer kan vi vara säkra på att även om informationen kommer i orätta händer så är den oläslig för obehöriga.

## 9.1 Kryptografiska säkerhetsåtgärder

Kryptografiska säkerhetsåtgärder syftar till att säkerställa korrekt och verkningsfull användning av kryptering för att skydda informationens konfidentialitet, äkthet och riktighet, t ex:

- *Konfidentialitet*: användning av kryptering av information för att skydda känslig eller kritisk information som antingen lagras eller överförs;
- *Riktighet/äkthet*: användning av digitala signaturer eller ”autentiseringskoder för meddelanden” för att verifiera äktheten eller riktigheten hos lagrad eller vidarebefordrad känslig eller kritisk information;
- *Oavvislighet*: användning av kryptografiska tekniker för att ge belägg för förekomst eller avsaknad av en händelse eller handling;
- *Autentisering*: användning av kryptografiska tekniker för att autentisera användare och andra systemenheter som begär åtkomst till eller verksamhetsförbindelser med systemets användare, enheter och resurser.

### 9.1.1 Regler för användning av kryptografiska säkerhetsåtgärder

Vid införande av regler för kryptering bör följande övervägas:

- En ledningsstrategi för användning av kryptografiska säkerhetsåtgärder som inkluderar hela organisationen inklusive allmänna principer enligt vilka verksamhetsinformation ska skyddas;
- Den skyddsnivå som krävs bör fastställas baserat på informationsklassning och riskbedömning och med hänsyn tagen till typ, styrka och kvalitet på den krypteringsalgoritm som krävs;
- Användning av kryptering för skydd av information som överförs på mobila enheter eller flyttbara medieenheter eller över kommunikationslinjer.
- En strategi för nyckelhantering, inklusive metoder för att hantera skyddet av kryptografiska nycklar och återvinning av krypterad information om nycklar förloras, äventyras eller skadas;
- Roller och ansvar, t ex vem som ansvarar för:
    - Införande av regler
    - Central förvaltning inklusive nyckelgenerering (se *9.1.2 Nyckelhantering*);
- Vilka standarder som bör införas för verkningsfullt genomförande i hela organisationen (vilken lösning som används för vilka verksamhetsprocesser);
- Effekten av att använda krypterad information på säkerhetsåtgärder som är beroende av att innehållet inspekteras (t ex upptäckt av skadlig kod).

*Kommentar:* Ett beslut om huruvida en krypteringslösning är lämplig bör ses som en del av den bredare processen för riskbedömning och val av säkerhetsåtgärder. Denna bedömning kan sedan användas för att avgöra huruvida en säkerhetsåtgärd baserad på kryptering är lämplig, vilken typ av säkerhetsåtgärd som bör tillämpas och för vilket syfte och för vilka verksamhetsprocesser.

Regler för användning av säkerhetsåtgärder baserade på kryptering är nödvändiga för att maximera nytta och minimera riskerna med att använda krypteringsteknik och att undvika olämplig eller felaktig användning.

### 9.1.2 Nyckelhantering

Regler för användning, skydd och giltighetstid för kryptografiska nycklar och för deras hela livscykel bör utvecklas och införas.

Reglerna bör omfatta krav för hantering av krypteringsnycklar avseende deras hela livscykel inklusive generering, lagring, arkivering, hämtning, distribution, återkallande och destruering av nycklar.

Kryptografiska algoritmer, nyckellängder och praktisk användning bör väljas enligt praxis. Lämplig nyckelhantering kräver säkra processer för att generera, lagra, arkivera, hämta, distribuera, återkalla och förstöra kryptografiska nycklar.

Alla krypteringsnycklar bör skyddas mot förändring och förlust. Hemliga och privata nycklar måste dessutom skyddas mot obehörig användning och utlämnande. Utrustning som används för att skapa, lagra och arkivera nycklar bör skyddas fysiskt.

Ett system för nyckelhantering bör baseras på en överenskommen uppsättning standarder, rutiner och säkra metoder för att:

- Generera nycklar för olika kryptografiska system och tillämpningar;
- Utfärda och erhålla certifikat för offentlig nyckel;
- Distribuera nycklarna till avsedda enheter, inklusive hur nycklar bör aktiveras vid mottagande;
- Lagra nycklar, inklusive hur behöriga användare får tillgång till nycklar;
- Ändra eller uppdatera nyckel inklusive regler om när nycklar bör ändras och hur detta kommer att ske;
- Hantera komprometterade nycklar;
- Återkalla nycklar inklusive hur nycklarna bör återkallas eller avaktiveras, t ex när nycklar har komprometterats eller när en användare lämnar en organisation (i vilket fall nycklar också bör arkiveras);
- Säkerhetskopiera eller arkivera nycklar;
- Förstöra nycklar;
- Loggning och revision av till nyckelhanteringen relaterade aktiviteter.

För att minska risken för felaktig användning bör datum för aktivering och avaktivering definieras så att nyckeln endast kan användas under angiven tidsperiod i de aktuella reglerna för nyckelhantering.

Förutom att säkert hantera hemliga och privata nycklar bör även äktheten hos offentliga nycklar bedömas. Detta kan göras genom att använda certifikat för offentliga nycklar som normalt utfärdas av en certifikatutfärdare, som bör vara en betrodd organisation med lämpliga säkerhetsåtgärder och rutiner som ger den nödvändiga graden av förtroende.

Innehåll i överenskommelser om tjänsteleverans eller avtal med externa leverantörer av kryptografiska tjänster, t ex med en certifikatutfärdare, bör omfatta frågor om ansvar, tillförlitlighet och svarstider för tillhandahållande av tjänster

*Kommentar*: Hantering av krypteringsnycklar är avgörande för en verkningsfull användning av krypteringsteknik. Krypteringsteknik kan också användas för att skydda kryptografiska nycklar. Rutiner kan behöva övervägas för hantering av förelägganden från myndigheter om åtkomst till kryptografiska nycklar, t ex om krypterad information behöver göras tillgänglig i okrypterad form som bevis vid rättegång.

# 10 Driftsäkerhet

För att undvika störningar och driftstopp i Högsby kommuns IT-system måste det finnas en god förvaltning med noggranna rutiner för till exempel driftsättning, säkerhetskopiering och loggning. När IT-driften sköts genom extern leverantör måste samma krav gälla som när driften sköts i egen regi.

## 10.1 Generella krav på systemmiljö

Högsby kommuns systemmiljö ska skyddas enligt instruktioner som fastställs inom respektive förvaltning och bolag.

Högsby kommun ska ha en systemmiljö med åtskilda produktions-, utvecklings-, test- och utbildningsmiljöer. Säkerhetsreglerna för produktionsmiljöer ska i relevanta delar även gälla för utvecklings- och testmiljöer. Utvecklingssystem ska i första hand hanteras i system eller datorprocesser och i domäner eller kataloger som inte hanterar produktionssystem.

Ändringar av produktionssystem och program ska i första hand testas i en test- eller mellanstationsmiljö innan överföring till driftsmiljö. Testning i produktionssystem får inte göras annat än i undantagsfall och då först efter godkännande av system- och informationsägare.

Högsby kommun ska ha en systemmiljö där industriella informations- och styrsystem, så kallade SCADA-system, endast i undantagsfall integreras med övriga IT-system. SCADA-system och anslutningar till dem ska kartläggas.

IT-system som ansluts till något av Högsby kommuns nätverk eller till nätverksansluten utrustning är konfigurerad enligt lokalt definierade standardkonfigurationer, vilka även ska ge användaren möjlighet att lagra information på gemensamma lagringsmedia.

## 10.2 Systemförvaltning

För att upprätthålla säker och tillförlitlig tillgång till information, ska administration, drift och underhåll av IT-system ske på ett strukturerat och systematiskt sätt, enligt en fastställd modell för systemförvaltning.

IT-system ska ha fastställda och aktuella rutiner för administration, drift och underhåll, dokumenterade i en systemförvaltningsplan. Planen ska säkerställa att systemen hanteras på ett enhetligt och informationssäkerhetsmässigt korrekt sätt och att beroendet av enskilda personers kunskaper minskas.

Beskrivning av IT-systems ändamål, säkerhetsklass och allmänna säkerhetsmål ska finnas dokumenterade och hållas aktuella.

Hot-, risk- och sårbarhetsanalyser ska genomföras regelbundet och innan viktiga förändringar genomförs, för att utvärdera om ett IT-systems säkerhetsskydd är tillfredsställande. Utifrån dessa analyser ska lämpliga skyddsåtgärder vidtas för att fastställd skyddsnivå ska få avsedd effekt. Analyserna ska kompletteras med en uppföljning av att systemen följer interna och juridiska krav.

## 10.3 Systemdokumentation

Det ska finnas systemdokumentation för varje IT-system. Dokumentationen ska normalt bestå av system-, drift- och användardokumentation, och utformas enligt gällande förvaltnings styrningsmodell.

### 10.3.1 Särskilda riktlinjer för systemdokumentation

Systemdokumentation ska vara fullständig och aktuell. Ändringar av dokumentationen, och kopior av dessa, ska ske enligt fastställda rutiner.

Det ska finnas en kopia av systemdokumentationen, liksom av andra för systemets användning och drift viktiga dokument. Dessa kopior ska förvaras skilda från originalen i brandcell eller annan byggnad.

Delar av systemdokumentationen som innehåller känslig information, till exempel om systemets säkerhetsfunktioner, ska förvaras så att den endast är åtkomlig för behörig personal.

I systemdokumentationen ska det framgå hur informationen ska bevaras och gallras samt vilken bevarande- och gallringsplan som gäller för systemet.

Arkivering av systemdokumentation ska ske i enlighet med Högsby kommuns arkivreglemente och legala krav.

## 10.4 Säkerhetsuppdateringar

Leverantörers säkerhetsuppdateringar ska installeras skyndsamt. För att säkerställa att driften inte påverkas negativt ska säkerhetsuppdateringarna testas och analyseras innan de installeras i produktionsmiljön. Om en uppdatering är så oundgänglig att det inte finns tid för tester ska den ske enligt fastställd rutin.

Se även *10.6 Styrning av ändringar i eller kring IT-system*.

## 10.5 Skydd mot skadlig kod

IT-system och utrustning som kan drabbas av datavirus eller annan skadlig kod, ska skyddas. Kontrollen ska vara obligatorisk och ske regelbundet och automatiskt. Definitionsfiler ska automatiskt uppdateras löpande, för att garantera generellt och aktuellt skydd.

Anvisningar och instruktioner för hantering av skydd och incidenter med anknytning till skadlig kod ska fastställas. Dessa ska innefatta instruktioner för hur användare ska identifiera, åtgärda och rapportera möjliga virusangrepp. Följande insatser bör mot bakgrund av ovanstående övervägas:

- Upprätta en formell regel som förbjuder användningen av icke-auktoriserade program
- Införa säkerhetsåtgärder som förhindrar eller upptäcker obehöriga program
- Införa säkerhetsåtgärder som förhindrar eller upptäcker användning av kända eller misstänkta skadliga webbplatser

- Upprätta en formell regel för skydd mot risker i samband med erhållande av filer och program från eller via externa nätverk eller andra medium som anger vilka skyddsåtgärder som bör vidtas
- Förbereda lämpliga kontinuitetsplaner för återhämtning från attacker orsakade av skadlig kod (se *14 Kontinuitetsplanering*)
- Isolera miljöer där påverkan kan vara katastrofal

För att förbättra skyddet mot skadlig kod är det lämpligt att använda två eller flera program från olika leverantörer och med olika teknik som skydd mot skadliga program i hela informationsbehandlingsmiljön.

Extra försiktighet bör vidtas för skydd mot skadlig kod vid underhåll och akuta åtgärder, då normala säkerhetsåtgärder kan komma att kringgås.

Förekomst av skadlig kod är att beteckna som informationssäkerhetsincident (*se 15.1 Incidentrapportering*) och ska rapporteras i enlighet med gällande rutin.

## 10.6 Styrning av ändringar i eller kring IT-system

Samtliga ändringar ska kunna härledas till en ansvarig beställare.

Formella rutiner ska fastställas för ändringshantering och testning inklusive godkännande av föreslagna förändringar, och ska vara kända av berörda personer. Rutinerna ska även säkerställa att det är möjligt att återgå till läget före ändringen.

Ändringar i eller kring ett IT-system ska planeras noga. Innan ändringsbeslut fattas ska analys av risker, sårbarheter och möjliga konsekvenser med avseende på fastställt ändamål, säkerhetsklass och säkerhetsmål göras.

Beslut om ändringar i eller kring ett IT-system ska fattas av systemägaren i enlighet med informationsägarens fastställda krav gällande ändamål och informationssäkerhet. Beslut om ändringar som väsentligen avviker från fastställt ändamål eller säkerhetsmål för IT-system eller på annat sätt kan påverka informationssäkerheten ska fattas av informationsägaren.

Ändringar, som bedöms kunna påverka informationssäkerheten, ska testas i separat testmiljö innan de införs i produktionsmiljö. Detta gäller för både rättningar av program och uppdateringar.

Om automatiska uppdateringar övervägs bör risk för förlust av riktighet och tillgänglighet vägas mot förmån för snabb distribution av uppdateringar. Automatiska uppdateringar bör inte användas på kritiska system då vissa uppdateringar kan orsaka att kritiska program upphör att fungera.

## 10.7 Felhantering

Allvarliga störningar i produktionsmiljö kräver ofta att åtgärder genomförs omgående och att fastställda rutinerna för ändringshantering inte kan följas. Sådana akuta ändringar ska dokumenteras och i efterhand följas upp enligt rutinen för ändringshantering.

## 10.8 Kapacitetsplanering

Kapacitetsplanering som syftar till att förutse och förebygga kapacitets- eller prestandaproblem i IT-miljö ska ske. Regelbunden mätning och uppföljning av kapaciteten ska genomföras. Detta är särskilt viktigt för de system som bedömts som verksamhetskritiska. Upptäckande åtgärder bör införas för att indikera problem i god tid. Det är viktigt att tillhandahålla prognoser för framtida kapacitetskrav som

tar hänsyn till ny verksamhet och systemkrav samt nuvarande och förutspådda trender i organisationens kapacitet för informationsbehandling.

Optimering och övervakning av system bör säkerställa och förbättra, där så är nödvändigt, tillgången till, och effektiviteten i systemen. Tillhandahållandet av tillräcklig kapacitet kan uppnås genom att öka kapaciteten eller genom att minska efterfrågan, vilket exempelvis kan ske genom att:

- ta bort föråldrade data (diskutrymme);
- avveckla tillämpningar, system, databaser eller miljöer;
- optimera batchprocesser och scheman;
- optimera logiken i tillämpningar eller databasfrågor;
- neka eller begränsa bandbredd för resurskrävande tjänster om dessa inte är verksamhetskritiska (t ex strömmande video).

## 10.9 Säkerhetskopiering och återläsning av data

Säkerhetskopiering av information och programvara ska utföras regelbundet, med frekvens och omfattning anpassad till verksamhetskrav respektive legala krav, enligt regler fastställda av Högsby kommun.

Korrekta och fullständiga register över säkerhetskopior och dokumenterade återställanderutiner ska utarbetas.

Tester för att återskapa information från säkerhetskopior ska genomföras regelbundet för att säkerställa att de kan användas samt för att testa återställanderutinerna. Testerna ska genomföras på dedikerad media och inte genom att skriva över den ursprungliga lagringsmedian, då det skulle kunna resultera i oreparerbar skada eller förlust av data i de fall säkerhetskopieringen eller återställningen misslyckas. Resultatet ska dokumenteras.

Säkerhetskopior och original ska förvaras i olika byggnader eller brandceller och med skyddsåtgärder som överensstämmer med informationens klassificering.

Driftsrutiner ska inbegripa övervakning av säkerhetskopiering, hantera fel vid schemalagda säkerhetskopieringar, samt säkerställa att säkerhetskopieringen är fullständig enligt reglerna för säkerhetskopiering.

Säkerhetskopiering för enskilda system och tjänster ska testas regelbundet för att säkerställa att de uppfyller kraven i kontinuitetsplaner. För kritiska system och tjänster ska säkerhetskopiering omfatta all information, alla program och all data som krävs för att återställa hela systemet i händelse av katastrof.

## 10.10 Driftövervakning

IT- system som är verksamhetskritiska ska driftövervakas kontinuerligt och loggas för att minimera avbrott och andra IT-incidenter. Loggar ska skyddas mot radering, manipulation och obehörig åtkomst.

Behovet av och rutiner för loggning och uppföljning av loggar (analys) ska fastställas av systemägaren i enlighet med verksamhetens behov och informationsklassificering. Lagkrav som är tillämpliga på övervakningsaktiviteterna ska följas. Områden som ska övervägas är till exempel behörig åtkomst,

privilegierade aktiviteter, obehöriga åtkomstförsök, systemlarm, ändringar eller försök till ändringar av IT-systems säkerhetsuppsättningar.

*Kommentar:* Bland de säkerhetskrav som finns för att skydda personuppgifter inom hälso- och sjukvård är de som är knutna till revision och loggning bland de viktigaste. Syftet är att säkerställa att spårbarhet för brukare som anförtror sin information till datajournaler och att kontrollera att åtkomstprivilegier inte missbrukas.

## 10.11 Drift hos extern part

När en verksamhet inom Högsby kommun köper IT som tjänst hos extern part eller förlägger drift av IT-system hos en sådan, ska minst samma regler för informationssäkerhet gälla som när driften hanteras i egen regi. Dessa krav ska definieras utifrån legala krav samt en dokumenterad risk- och sårbarhetsanalys.

Kraven på informationssäkerhet ska regleras i avtalet mellan parterna och uppföljning av avtalad säkerhetsnivå ska ske. Detta ska göras möjligt genom att i avtalet specificera att Högsby kommun har rättighet att genomföra revision av informationssäkerheten. Övervakning och granskning av leverantörstjänster bör säkerställa att informationssäkerhetsvillkor och bestämmelser i avtalen följs och att informationssäkerhetsincidenter och problem hanteras korrekt.

Om informationen i systemen innehåller personuppgifter ska parternas roller som personuppgiftsansvarig och personupppgiftsbiträde regleras i avtal i enlighet med dataskyddsförordningen (GDPR). I detta så kallade personuppgiftsbiträdesavtal ska det särskilt föreskrivas att personuppgiftsbiträdet bara får behandla personuppgifterna i enlighet med instruktioner från den personuppgiftsansvarige och att biträdet måste vidta lämpliga tekniska och organisatoriska åtgärder för att skydda personuppgifterna.

Risker som följer av beroendet av en viss leverantör ska minimeras och åtgärder vidtas för att hantera konsekvenserna av att en leverantör inte kan fullfölja sitt uppdrag.

### 10.11.1 Särskilda riktlinjer för molntjänster

IT-system som innehåller känslig information i klassen K3 eller högre enligt Högsby kommuns informationsklassningsmodell eller behöver integreras med andra IT-system ska inte upphandlas som en molntjänst utan att en noggrann risk- och sårbarhetsanalys först har genomförts och dokumenterats och erforderliga skyddsåtgärder vidtagits.

Om personuppgifter kommer att behandlas i ett land utanför EU/EES ska den personuppgiftsansvarige se till att något av undantagen från förbudet mot överföring till tredje land kan tillämpas.

Molntjänst ska som grundregel inte upphandlas om det är oklart var personuppgifter kommer att lagras eller bearbetas rent fysiskt (och därmed även geografiskt).

Kommentar: Nämnd eller styrelse som inom sitt ansvarsområde använder en molntjänst för sin personuppgiftsbehandling är personuppgiftsansvarig för behandlingen, även om den utförs av molntjänstleverantör eller dess underleverantörer. Om en leverantör anlitas för behandlingen, är denne och alla dess underleverantörer den personuppgiftsansvariges personuppgiftsbiträde.

## 10.12 Gallring av information och avveckling av IT-system

Gallring av information och avveckling av IT-system ska ske på ett säkert sätt och i enlighet med Högsby kommuns informationshanteringsplan och föreskrifter.

Det ska finnas instruktioner och rutiner för IT-utrustning som ska utrangeras, kasseras, säljas eller på annat sätt lämna myndigheten.

*Kommentar:* Lagringsmedia som innehåller känslig information eller licensierade program, ska förstöras, avmagnetiseras eller överskrivas på ett säkert sätt, i samband med avveckling eller återanvändning. Vid avveckling ska rättsliga regler såsom dataskyddsförordningen och arkivlagen uppmärksammas särskilt.

# 11 Kommunikations- och nätverkssäkerhet

Det finns alltid risker för avlyssning, intrång och för att den överförda informationen förändras när information överförs genom data- och telekommunikation. Trådlösa anslutningspunkter kan öppna det interna nätverket för omvärlden och orsaka stora problem om inte säkerhetskraven följs. Därför är säkerhetskraven höga på nätverksmiljön. Hur vi skyddar våra nätverk beskrivs i detta kapitel.

## 11.1 Säkerhetskrav på nätverksmiljön

Nätverk ska vara logiskt separerade. Varje nätverk ska utformas så att det finns definierade gränssnitt, såväl fysiskt som logiskt, mot andra nätverk.

För alla kommunala förvaltningar och bolag som nyttjar hk.hogsby.se ska anslutningar från det egna nätverket till andra nätverk och till internet ske via hk.hogsby.se. Om privata verksamheter med egen internetkoppling ska anslutas till kommunnäten fordras att riskanalys utförs och att särskild överenskommelse tecknas som reglerar det gemensamma nättrafikskyddet.

Respektive nätverk bör vara uppdelat i nätverkssegment för att minimera risken för obehörig åtkomst samt möjliggöra uppdelning i åtskilda produktions-, utvecklings- och testmiljöer. Utvecklings- och testarbete ska inte kunna störa produktionen.

Publika nätverk ska vara åtminstone logiskt separerade från verksamhetens allmänna nätverk.

Sammankoppling av nätverk får endast ske efter genomförd riskanalys och sedan nödvändiga skyddsåtgärder vidtagits av respektive nätverks systemägare. Sammankoppling med nät hos leverantörer ska godkännas av kommunchef eller av denne delegerad ansvarig.

Respektive nätverks systemägare ansvarar för att utifrån berörda informationstillgångar klassificering analysera behov av, införa och dokumentera nödvändiga skyddsåtgärder för att hantera risk för avlyssning och förändring av överförd information.

Respektive nätverks systemägare ska utifrån informationsägarnas krav på tillgänglighet och säkerhet besluta om nätverksinfrastruktur och val av aktiva nätkomponenter.

Respektive nätverks systemägare ska se till att det finns anslutningsbestämmelser för nätverket, framförallt bör system i nätverket autentiseras och systemanslutningar till nätverket begränsas.

Nätverk, dess komponenter och systemsamband ska vara dokumenterade. Det innebär att det ska finnas systemskisser över samtliga komponenter ingående i hk.hogsby.se och olika LAN-lösningar samt att alla anslutningspunkter gentemot andra nätverk är tydligt utmärkta.

Fjärranslutningar till IT-system för till exempel fjärrdiagnostik eller -övervakning ska ske genom hk.hogsby.se och under kontrollerade och säkra former fastställda av respektive systemägare.

## 11.2 Särskilda riktlinjer för trådlösa nätverk

I samband med att information överförs med hjälp av trådlösa kommunikationsnätverk, uppkommer risker som kräver ytterligare skyddsåtgärder. Den påtagliga risken för avlyssning kräver att denna kommunikation krypteras.

Kommunchefen eller av denne delegerad ansvarig ska fastställa anvisningar och instruktioner för design, konfiguration och användning av trådlösa nätverk.

Vid användning av trådlösa nätverk ska risken för störningar mot IT-system och känslig utrustning, som till exempel medicinteknisk utrustning, beaktas.

Kommentar: Ytterligare krav som berör elektroniska kommunikationsnät finns i kapitlet *7 Användning av IT-system*.

# 12 Utveckling och anskaffning av IT-system

Vilka informationssäkerhetskrav gäller när informationssystem ska utvecklas eller anskaffas? Tryckfrihetsförordningen, offentlighets- och sekretesslagen, arkivlagen, dataskyddsförordningen, lagen om offentlig upphandling och våra egna verksamheter ställer alla krav som måste analyseras vid utveckling eller upphandling. Hur dessa frågor hanteras beskrivs i detta kapitel.

## 12.1 Generella regler vid utveckling och anskaffning

Vid utveckling och anskaffning av IT-system ska det noga analyseras vilket säkerhetsskydd systemet kräver och vilka åtgärder som måste vidtas för att säkerhetsskyddet ska få avsedd effekt. Kraven på systemet ska tydligt framgå i kravspecifikationen.

Vid utveckling och anskaffning av IT-system ska det, om det är behövligt, finnas en IT-säkerhetsansvarig som leder och samordnar IT-säkerhetsarbetet. Utvecklingens eller anskaffningens omfattning får avgöra om det behöver finnas en sådan.

IT-systemet ska, innan det tas i drift, ha godkänts ur säkerhetssynpunkt av den för vars verksamhet systemet inrättas.

En formell process för testning och anskaffning ska följas när produkter anskaffas. Avtal med leverantörer ska behandla de identifierade säkerhetskraven. Då säkerhetsfunktionen i en föreslagen produkt inte uppfyller angivna krav ska den tillkommande risken och säkerhetsåtgärder som är relaterade till den analyseras innan produkten anskaffas.

Godkännandekriterier för produkter bör fastställas t ex när det gäller deras funktionalitet som kommer att bekräfta om identifierade säkerhetskrav uppfylls. Produkter bör utvärderas mot dessa kriterier innan anskaffning. Tillkommande funktionalitet bör utvärderas för att säkerställa att det inte medför nya oacceptabla risker.

IT-system ska, innan de tas i drift, vara informationssäkerhetsklassificerade enligt Högsby kommuns gällande klassificeringsmodell.

Kommentar: Vid upphandling, ny- och vidareutveckling av IT-system, i egen regi eller i samverkan med samarbetspartner, ska informationssäkerhetskraven analyseras och definieras utifrån en väl dokumenterad hot- och riskanalys, legala krav och informationsklassificering, allt i enlighet med tidigare nämnda krav i detta dokument. Det bör särskilt beaktas hur IT-systemet är avsett att samverka med andra IT-system. Det bör även särskilt beaktas hur informationen som IT-systemet ska hantera får bevaras eller gallras för att säkerställa att rätt information sparas den dag det ska avvecklas.

## 12.2 Systemutvecklingsprojekt

Det ska i systemutvecklingsprojekt tillses att dokumenterade modeller för systemutveckling och projektstyrning finns och tillämpas.

I systemutvecklingsprojekt ska system, programvara och informationstillgångar skyddas på motsvarande sätt som de färdiga produkterna. Produktionsmiljöer ska skyddas.

Information i samband med systemutveckling ska skyddas enligt samma principer som övrig verksamhetsinformation. Testmiljö ska, om inte särskilda skäl föreligger, inte innehålla produktionsdata. Användning av persondata som kan härledas till identifierbara personer eller information i informationssäkerhetsklasserna K3 eller högre enligt Högsby kommuns informationsklassningsmodell får inte förekomma i testmiljö.

Instruktioner för acceptanstest, driftgodkännande och produktionssättning ska finnas och tillämpas. System ska genomgå acceptanstest före godkännande av beställare. I godkännandet ska det ingå en uppföljning av säkerhetskraven. Ett beslut ska fattas om eventuella avvikelser hindrar en produktionssättning och inom vilken tidsram de ska åtgärdas. Är systemet godkänt kan det därefter överlämnas för produktionssättning.

## 12.3 Upphandling av IT-system och systemutveckling

Högsby kommuns riktlinjer för upphandling ska följas.

Informationssäkerhet och skyddskrav ska vara en naturlig del av ett anbud eller en upphandling.

En upphandling som inte innefattar hantering av sekretessbelagda uppgifter görs genom Högsby kommuns normala rutiner och i enlighet med lagen om offentlig upphandling, LOU. Högsby kommuns upphandlingspolicy ska följas och avrop mot befintliga ramavtal göras i första hand.

I kravspecifikationen ska alltid ingå de i riskanalysen fastlagda informationssäkerhetskraven och de legala kraven. Vidare ska en specifikation av i vilka tekniska miljöer och på vilka plattformar systemet ska fungera liksom krav på att systemets trafikkaraktäristik redovisas i anbudet.

### 12.3.1 Särskilda riktlinjer vid upphandling

I förfrågningsunderlaget ska de krav som ställs på leverantören anges. Det gäller såväl krav på leverantörens arbete med informationssäkerhet som ekonomiska, finansiella och tekniska förmågor.

Avtal ska utformas så att beställaren erhåller fullständigt ägande, förfogande och upphovsrätt samt övriga immateriella rättigheter till allt arbete och material som upp- eller tillkommit i samband med uppdraget. Om detta inte är möjligt bör avtal om deponering av källkod träffas. Fysiskt överlämnande till beställaren, så kallad tradition, måste ske för att besittningsövergång ska anses ha skett.

*Kommentar:* Högsby kommun ska sträva efter att få till stånd så kallad tradition av lös egendom, upphovsrätt till dataprogram och annat av immateriell rätt skyddat intellektuellt arbete, vilket tagits fram inom ramen för uppdraget. Det är nödvändigt för att skydda beställaren mot leverantörens borgenärer, i händelse av konkurs eller obestånd.

# 13 Leverantörsrelationer

## 13.1 Informationssäkerhet i leverantörsrelationer

Syftet med informationssäkerhet i leverantörsrelationer är att säkerställa skydd av de organisationstillgångar som leverantörer har åtkomst till.

### 13.1.1 Informationssäkerhetsregler för leverantörsrelationer

När kommunen köper IT-tjänster av extern part eller förlägger drift av informationssystem och tjänster hos en sådan, ska minst samma regler för informationssäkerhet gälla och avtalas som när driften hanteras i egen regi.

Information kan äventyras av leverantörer med otillräcklig styrning av informationssäkerhet. Säkerhetsåtgärder bör identifieras och användas för att administrera leverantörens tillgång till informationsbehandlingstjänster. Om det t ex finns ett särskilt behov av konfidentialitet för informationen, kan avtal om tystnadsplikt användas. Ett annat exempel är risker relaterade till skydd av data när leverantörsavtalet innebär överföring av, eller tillgång till, information över nationella gränser. Högsby kommun som organisation måste vara medveten om att det lagstadgade ansvaret eller avtalsenliga ansvaret för att skydda information kvarstår hos Högsby kommun.

### 13.1.2 Hantering av säkerhet inom leverantörsavtal

Alla relevanta informationssäkerhetskrav ska upprättas och avtalas med varje leverantör som kan tillgå, behandla, lagra och kommunicera information eller som tillhandahåller informationssystem och tjänster till kommunen.

Leverantörsavtal ska upprättas och dokumenteras för att säkerställa att det inte finns några missförstånd mellan Högsby kommun och leverantören avseende bägge parters skyldigheter att uppfylla relevanta informationssäkerhetskrav.

### 13.1.3 Försörjningskedja för informations- och kommunikationsteknologi

Avtal med leverantörer ska innehålla krav på att hantera informationssäkerhetsriskerna förknippade med försörjningskedjan för informationssystem, produkter och tjänster baserade på informations- och kommunikationsteknologi.

Med försörjningskedjan avses samtliga aktörer som är delaktiga i framtagande och leverans av informationssystem, produkter och tjänster.

# 14 Fysisk och miljörelaterad säkerhet

Tillträdeskontroll, säkra utrymmen, skalskydd och brandskydd – det är några av de rubriker som tas upp under denna rubrik, Fysisk säkerhet. Det handlar om hur IT-system och informationstillgångar ska skyddas, både i våra egna lokaler och när vi hyr in oss i andras.

## 14.1 Generella regler för fysisk och miljörelaterad säkerhet

Nivån på det fysiska skyddet av tillgångar ska baseras på genomförda riskanalyser och stå i proportion till identifierade risker. Grundregeln är att information aldrig ska lämnas oskyddad.

IT-system och utrustning som är känslig i sig själv eller behandlar känslig information, ska placeras så att tillträde minimeras och utformningen av lämpliga skyddsåtgärder underlättas.

Kritiska IT-system och viktiga informationstillgångar ska inrymmas i säkra utrymmen.

Tillträdeskontroll till viktiga byggnader och lokaler ska finnas, för att säkerställa att endast behörig personal ges tillträde.

Fysiska säkerhetsåtgärder för information, IT-system och utrustning ska samordnas med fysisk säkerhet och säkerhetsåtgärder för anställda och brukare där så är tillämpligt.

## 14.2 Säkra utrymmen

Med säkra utrymmen avses utrymmen som är speciellt planerade och uppbyggda för att uppfylla höga krav på otillåten åtkomst, skada och störning. Skydd av sådana utrymmen ska utformas i proportion till förekommande risker och ska omfatta skal och brandskydd, säkerhetsspärrar och tillträdeskontroller.

### 14.2.1 Fysiska säkerhetsavgränsningar

Skalskyddet ska anpassas till säkerhetskrav för tillgångarna inom skalskyddet och resultatet av en riskbedömning. Skalskyddet bör byggas upp i flera nivåer. Branschnormer ska följas.

För att säkerställa att endast behörig personal ges tillträde till säkrade utrymmen, ska dessa skyddas med hjälp av lämpliga tillträdesspärrar och -kontroller.

Entréer ska skyddas med bemannade receptioner eller datoriserade passagekontrollsystem. För att möjliggöra loggning av in- och utpasserande ska kontrollsystemen vara kopplade till individuella passagekort eller koder.

Om det i övrigt har installerats passagekontrollsystem, bör ur kostnads- och effektivitetssynpunkt också de säkra utrymmena anslutas till samma system. De speciella krav på begränsning av tillträdet som kan finnas, per individ, tid på dygnet etcetera, måste dock kunna tillgodoses. Fastställda rutiner för uppföljning av loggar ska finnas och tillämpas.

För att uppnå full effekt av tillträdesskyddet bör det integreras med inbrottslarm.

### 14.2.2 Fysiska tillträdesbegränsningar

Datum och tid för besökares ankomst och utgång bör registreras och alla besökare bör övervakas om inte deras tillträde har godkänts tidigare. Besökare bör även endast beviljas tillträde för specifika och godkända syften samt delges instruktioner avseende områdets säkerhetskrav och rutiner vid nödsituationer. Besökarnas identitet bör även säkerställas på lämpligt sätt.

Tillträde till områden där konfidentiell information bearbetas eller lagras bör begränsas till behöriga personer genom att införa lämpliga åtkomstkontroller, t ex genom att införa tvåfaktorsautentisering med mekanismer som passerkort eller hemliga PIN-koder, se även *12.2.1 Fysiska säkerhetsavgränsningar*.

En fysisk loggbok eller en elektronisk verifieringskedja över alla tillträden bör också underhållas och bevaras säkert.

Anställda, leverantörer och externa parter bör åläggas att bära någon form av synlig identifiering och samtidigt vara uppmärksamma på och omedelbart underrätta närmaste chef eller ansvarig kontaktperson om de möter besökare utan ledsagare eller någon synlig identifiering.

Extern servicepersonal bör beviljas begränsat tillträde till säkra områden eller områden där konfidentiell information bearbetas endast när så krävs. Detta tillträde bör också godkännas och övervakas.

## 14.3 Utrustning och skydd

IT-system och annan elektronisk utrustning är känsliga för brand, annan temperaturhöjning och rök. Det är viktigt att ett ändamålsenligt skydd finns i de utrymmen där sådan utrustning finns. Det är även lämpligt att har larm för att upptäcka sådana eventuella störningar. Expertis ska anlitas för att skapa rätt dimensionerat brandskydd.

Har IT-system och annan känslig utrustning utsatts för rök, öppen låga, vatten eller annan för utrustningen skadlig kemikalie, ska de saneras. Restvärdesföretag som har specialiserats på omhändertagande av utrustning och övriga inventarier ska användas, för att minska de totala skade- och försäkringskostnaderna.

Rör, där vatten står under tryck, bör inte finnas i säkra utrymmen. Vätskelarm ska finnas, om det i utrymmet finns rördragningar innehållande vatten, eller om det av andra orsaker finns risk för vattenskada.

Verksamhetskyla ska finnas som motsvarar den överskottsvärme som alstras av IT-system eller utrustning.

## 14.4 Kraftförsörjning och elmiljö

Verksamhetskritiska system och verksamhetsställen med starkt beroende av elförsörjning ska vara försedda med reservkraft.

IT-system och annan elektronisk utrustning bör skyddas mot elavbrott och andra störningar i elförsörjningen. Strömförsörjning av verksamhetskritiska system och utrustningar bör ske via avbrottsfri kraftmatning (UPS), som i sin tur bör anslutas till reservkraft.

Kablage för strömförsörjning bör hållas åtskilda från kommunikationskablage för att förhindra störningar.

Tester ska göras regelbundet för att säkerställa att övergången till reservkraft fungerar. Risker rörande den elektromagnetiska miljön bör beaktas.

## 14.5 Säkerhet för tillgångar utanför egna lokaler

Risker i samband med hantering av system och utrustning och andra tillgångar utanför de egna lokalerna ska beaktas och nödvändiga skyddsåtgärder vidtas. Instruktioner ska fastställas för sådan hantering.

*Kommentar:* Vid utformning av skyddsåtgärder måste det beaktas att säkerhetsrisker kan variera avsevärt mellan olika platser och vid olika tidpunkter. Viktigt är att även beakta riskerna då exempelvis utrustning lämnas ut för extern service.

# 15 Hantering av incidenter som rör informationssäkerhet

När en allvarlig incident inträffar som påverkar informationssäkerheten är det viktigt att vi agerar snabbt för att begränsa eller avvärja konsekvenserna av den. Störningar kan ha flera orsaker och kan snabbt komma att påverka många delar av vår verksamhet, men också andra aktörer i samhället. I detta kapitel behandlas hur vi hanterar sådana slags händelser.

## 15.1 Incidenthantering

Informationssäkerhetsincidenter ska hanteras enligt samma process som andra verksamhetsstörningar. Informationssäkerhetshändelser ska bedömas och beslut ska fattas om de klassas som informationssäkerhetsincidenter.

### 15.1.1 Ansvar och rutiner

Alla medarbetare och leverantörer som använder Högsby kommuns informationssystem och -tjänster ska rapportera avvikelser som kan utgöra ett hot mot Högsby kommuns informationssäkerhet i system och tjänster enligt anvisad rutin. Kommunchef/Förvaltningschef/VD ska tillsammans med Informationssäkerhetsstrateg fastställa rutin för hur sådan rapportering ska genomföras.

Rutin för rapportering av informationssäkerhetshändelser bör innefatta:

- Förberedda formulär för rapportering av informationssäkerhetshändelser i syfte att underlätta rapportering och för att hjälpa personen som lämnar rapporten att komma ihåg alla nödvändiga åtgärder vid en informationssäkerhetshändelse samt fastställande av kontaktpunkt för rapportering av informationssäkerhetshändelser;
- Tydliggörande av rutiner som bör följas vid en informationssäkerhetshändelse, t ex att omedelbart notera alla detaljer, såsom om händelsen innebär bristande efterlevnad eller överträdelse av regler, uppkomna fel, meddelanden på skärmen, samt omedelbar rapportering till Informationssäkerhetsstrateg och närmaste chef och endast genomföra koordinerade åtgärder;
- Lämpliga återkopplingsprocesser för att säkerställa att de personer som rapporterar informationssäkerhetshändelser underrättas om resultaten efter att frågan har behandlats och avslutats.

### 15.1.2 Rapportering av informationssäkerhetshändelser

Informationssäkerhetshändelser ska rapporteras enligt fastställd rutin så snabbt som möjligt. Informationssäkerhetshändelser som bör övervägas att rapporteras inkluderar:

- Säkerhetsåtgärder utan verkan;
- Avsteg från förväntningar på informationens riktighet, konfidentialitet, och tillgänglighet;
- Mänskliga fel
- Bristande efterlevnad av policy, regler och riktlinjer;
- Överträdelser av fysiska skyddsåtgärder;
- Okontrollerade systemförändringar;
- Fel i program och hårdvara;
- Överträdelse av åtkomstregler.

*Övrig information*

Störningar eller andra onormala beteenden i system kan vara en indikator på ett angrepp eller faktiska säkerhetsbrister och bör därför alltid rapporteras som en informationssäkerhetshändelse.

### 15.1.3 Bedömning av och beslut om informationssäkerhetshändelser

Högsby kommuns Informationssäkerhetsstrateg ska utvärdera varje informationssäkerhetshändelse utifrån en överenskommen skala för klassning av informationssäkerhetshändelser och incidenter. Informationssäkerhetsstrategen beslutar också om huruvida händelsen ska klassas som en informationssäkerhetsincident eller ej.

Akuta IT-incidenter som kräver omedelbara åtgärder ska rapporteras till IT-driftorganisationen, till exempel via verksamhetens IT-support. IT-incidenter som innebär att en utrednings- eller åtgärdsfas behöver påbörjas ska snarast rapporteras till närmaste chef och till verksamhetens informationssäkerhetsrepresentant enligt anvisade rutiner.

### 15.1.4 Hantering av informationssäkerhetsincidenter

Det ska finnas en rutin för hur informationssäkerhetsincidenter hanteras inom Högsby kommun.

Hanteringen av informationssäkerhetsincidenter bör inkludera följande:

- Insamling av bevis så snart som möjligt efter inträffande
- Möjlighet till genomförande av en forensisk analys, om så krävs, vilket innebär att det ska finnas rutiner för att hantera bevis i syfte att vidta disciplinära och rättsliga åtgärder. Rutinerna för hantering av bevis bör ta hänsyn till:
    - Spårbarhet
    - Säkerhet för bevis
    - Säkerheten för personalen
    - Roller och ansvar för involverad personal
    - Kompetensen hos personalen
    - Dokumenterad information
    - Delgivning
- Eskalering efter behov
- Säkerställande av att alla aktiviteter loggas korrekt för senare analys
- Kommunikation av informationssäkerhetsincidenten eller relevanta detaljer kopplade till incidenten till interna eller externa personer eller organisationer som behöver informeras

- Hantering av brister i informationssäkerheten som har konstaterats orsaka eller bidragit till händelsen
- När incidenten har hanterats tillfredsställande bör ärendet formellt avslutas och dokumenteras

En fördjupad analys efter incidenten bör, vid behov, genomföras för att identifiera orsaken till incidenten. Den kunskap som analysen av hanterande informationssäkerhetsincidenter ger bör användas för att minska sannolikheten eller påverkan av framtida incidenter.

Det bör finnas processer som möjliggör kvantifiering och övervakning av typer, omfattning och kostnader avseende informationssäkerhetsincidenter. Informationen som erhålls från utvärderingen av informationssäkerhetsincidenter bör användas för att identifiera återkommande incidenter eller incidenter med stor påverkan. Utvärderingen kan även indikera behov av förbättrade eller kompletterande säkerhetsåtgärder för att begränsa frekvensen, skador och framtida händelser.

*Kommentar:* Informationssäkerhetsincidenter är oavsiktliga eller avsiktliga händelser och risker som påverkar eller kan komma att påverka säkerheten negativt för Högsby kommuns informationstillgångar. Exempel på sådana incidenter är brott mot sekretessen, allvarliga driftavbrott, skadlig kod eller programvara, dataintrång eller obehörigt användande av information. Incidenter kan även vara förlust av dator eller lagringsmedia. Mer information kan lämnas av Högsby kommuns Informationssäkerhetsstrateg.

När en informationssäkerhetshändelse upptäcks, är det inte alltid uppenbart om händelsen kommer att resultera i rättsliga åtgärder. Därför finns det en risk att nödvändiga bevis avsiktligt, eller oavsiktligt, förstörs innan allvarlighetsgraden i händelsen är helt klarlagd. Det är lämpligt att kontakta en jurist eller polisen tidigt vid planerade rättsliga åtgärder och rådfråga dem avseende de bevis som krävs.

# 16 Kontinuitetsplanering

Verksamheten ska kunna fortsätta även om till exempel IT-system slås ut, en strömkabel grävs av eller byggnader brinner ner. Därför är det viktigt att planera också hur verksamheten ska fungera om det händer något. Här finns riktlinjerna för hur vi gör det och planerar för kontinuitet.

## 16.1 Generella regler för kontinuitetsplanering

Informationssäkerhet ska vara en integrerad del av den överordnade processen för verksamhetens kontinuitetsplanering. Processen ska behandla nödvändiga informationssäkerhetskrav som behövs för verksamheten i kontinuitet.

I verksamhetens kontinuitetsplan ska det behandlas hur verksamheten ska bedrivas vid avsaknad av kritiska funktioner, informationstillgångar och IT-system samt hur återgång till normalläge ska ske.

Kontinuitetsplaner och återstartsplaner skall finnas för all information och alla system som klassats i tillgänglighetsklass T3 eller högre enligt Högsby kommuns klassificeringsmodell, se tillämpningsanvisning ”Informationsklassning – Högsby kommun”. Planer kan vara gemensamma för flera verksamheter och flera system och ska innehålla fastställda prioriteringsordningar för återgång till normalläge.

Målet med kontinuitetsplaneringen ska vara att kritiska verksamheter ska kunna upprätthållas, på rimlig nivå, vid olika typer av katastrofsituationer, störningar och oplanerade avbrott. De delar av kontinuitetsplaneringen som berör katastrof- och beredskapssituationer ska ingå i verksamhetens övriga katastrofplanering.

Det ska finnas fastställda och aktuella reservrutiner för katastrofsituationer, störningar eller oplanerade avbrott. Rutinerna kan vara såväl manuella som IT-baserade.

Kontinuitetsplanerna ska testas regelbundet, minst årligen, enligt fastställd plan samt efter större organisationsförändringar. Planerna ska underhållas genom regelbundna granskningar och övningar, för att säkerställa att de är aktuella och ändamålsenliga.

*Kommentar:* Det är viktigt att fastställa rätt nivå för varje verksamhet, det vill säga hur länge ett eventuellt stillestånd accepteras eller om verksamheten endast behöver fungera delvis under en tidsperiod. För att hitta rätt ambitionsnivå måste juridiska krav samt verksamhetens behov av tillgång till information dokumenteras och riskanalyser genomföras. Kontinuitetsplanerna ska innefatta reservrutiner och övriga åtgärder som i förväg kan vidtas för att säkerställa verksamhetens kontinuitet. Om verksamheten är beroende av en annan organisation som till exempel en IT-leverantör måste även den vara involverad i arbetet. Förordning (2002:472) om åtgärder för fredstida krishantering och höjd beredskap ställer särskilda krav på verksamheten vid beredskapsmyndigheter.

## 16.2 Redundans

Informationssystem och -tjänster bör vid införande uppfylla krav på tillgänglighet.

Verksamhetskrav bör identifieras avseende tillgänglighet till informationssystem och -tjänster. Där tillgången till systemet eller tjänsten inte kan garanteras med hjälp av den befintliga systemarkitekturen bör redundanta enheter eller redundant arkitektur övervägas.

I tillämpliga fall bör även redundanta informationssystem testas för att säkerställa att övergången från en enhet till en annan fungerar som avsett.

Införandet av redundans kan medföra risker avseende riktighet och konfidentialitet för information och informationssystem, vilket bör beaktas vid utformningen av informationssystem.

# 17 Uppföljning och efterlevnad

Här får vi veta hur och när vi ska göra uppföljningar så att vi vet vad som fungerar bra och vad vi behöver förändra för att hålla en god informationssäkerhet och samtidigt uppfylla den demokratiska uppgift vi har som offentlig myndighet.

## 17.1 Uppföljning av regelverket

Kommunchefen ska, på informationssäkerhetsstrategens initiativ, inleda ett ärende om ändring av informationssäkerhetspolicyn eller av dessa riktlinjer.

Anpassningar av Högsby kommuns regelverk för informationssäkerhet ska ske utifrån bland annat resultat från risk- och sårbarhetsanalyser samt omvärlds- och verksamhetsanalyser.

## 17.2 Uppföljning av efterlevnad

Informationssäkerheten ska enligt Högsby kommuns informationssäkerhetspolicy följas upp regelbundet.

Kommunstyrelsen har det övergripande ansvaret för informationssäkerheten inom Högsby kommun och därmed för samordning och uppföljning av denna.

Varje nämnd och styrelse är ytterst ansvarig för informationssäkerheten inom sin förvaltning respektive bolag. Det åligger varje nämnd och styrelse att löpande följa upp informationssäkerheten och i övrigt vidta de åtgärder som krävs för att uppnå och upprätthålla tillräcklig intern kontroll.

Varje förvaltning och bolag ska regelbundet granska sin informationssäkerhet och därvid inventera installerade system samt göra en analys av hur systemen förhåller sig till författningar, dessa riktlinjer och tillhörande tillämpningsanvisningar, verksamhetens lokala styrdokument för informationssäkerhet samt andra regler som styr verksamheten. Baserat på genomförda granskningar och identifierade avvikelser ska skyddsåtgärder vidtas, anpassas och kompletteras.

För att säkerställa att regelverket efterlevs ska granskningar genomföras årligen, och när det inträffar väsentliga händelser som påverkar informationssäkerheten. Dessa kan initieras av Högsby kommuns Informationssäkerhetsstrateg eller av Högsby kommuns revisorer; på eget initiativ eller inom ramen för en planerad revision.

Varje år ska Informationssäkerhetsstrategen rapportera arbetet med informationssäkerheten till Kommunchefen, vilket beskrivs under *4.1 Roller och ansvar i verksamheten*.

Efterlevnaden av Högsby kommuns riktlinjer för informationssäkerhet ska årligen följas upp på en övergripande nivå genom informationssäkerhetsrådet och rapporteras till kommunchefen via Informationssäkerhetsstrategen, se även *4.4 Roller och ansvar gällande samordning och uppföljning*.