STRATEGI
PROGRAM
PLAN
POLICY
RIKTLINJER
REGLER

RIKTLINJER FÖR INFORMATIONS-SÄKERHET

HÖGANÄS KOMMUN

Fastställt av: Kommunfullmäktige
Datum: 2022-04-12
För revidering ansvarar: Informationssäkerhetsansvarig
För eventuell uppföljning och tidplan ansvarar: Informationssäkerhetsansvarig
Dokumentet gäller för: Samtliga förvaltningar och kommunala bolag
Dokumentet gäller till och med: Tills vidare

Innehållsförteckning

1 OMFATTNING

Riktlinjerna för informationssäkerhet är en konkretisering av Höganäs kommuns policy för informationssäkerhet och personuppgiftshantering KS/2019/255 och anger hur information ska hanteras inom kommunkoncernen. Dessa riktlinjer gäller för alla verksamheter vilket innebär att det inte finns utrymme att besluta om lokala avvikelser, enbart lokala tillägg specifika för verksamheten. Riktlinjerna kompletteras av regler för informationssäkerhet.

Alla medarbetare inom kommunkoncernen ska regelbundet informeras om och utbildas i innehållet i riktlinjer och regler för informationssäkerhet enligt fastställd utbildningsplan.

Bestämmelserna i riktlinjerna omfattar även externa parter som arbetar på uppdrag åt Höganäs kommunkoncern, exempelvis konsulter eller inhyrd kompetens.

För extern part ansvarar den person som tecknar avtal med den externa resursen för att informationen kommer denna till del. Policy för informationssäkerhet och personuppgiftshantering konkretiseras även i riktlinjer för personuppgiftshantering med tillhörande regler och rutiner.

Säkerhetsskyddsklassificerade uppgifter enligt säkerhetsskyddslag (2018:585) omfattas inte av bestämmelserna i dessa riktlinjer, för dessa finns en särskild säkerhetsskyddsanalys[1] och säkerhetsskyddsplan[2].

1.1 STRUKTUR OCH LÄSANVISNINGAR

För att ge god läsbarhet är dokumentet uppdelat i fem kapitel som riktar sig till olika målgrupper.

KAPITEL		INNEHÅLL	PRIMÄR MÅLGRUPP
1	Omfattning	Introduktion informationssäkerhet	Alla medarbetare
2	Styrning och ansvar	Roller och ansvarsfördelning för informationssäkerhet. Information och riktlinjer för hur arbetet med informationssäkerhet ska bedrivas	Alla medarbetare
3	Informationssäkerhet för medarbetare	Information, riktlinjer och regler för hur information ska hanteras i olika situationer	Alla medarbetare
4	Informationssäkerhet i verksamhet	Information och riktlinjer för Informationssäkerhet för hur information ska hanteras inom verksamhet och förvaltning.	Chef, informationsägare, systemägare samt roller för systemförvaltning
5	Informationssäkerhet i IT-miljön	Information och riktlinjer för hur informationssäkerhet ska hanteras inom IT-miljön.	Chef, informationsägare, systemägare samt roller för systemförvaltning

1.2 BILAGOR

Riktlinjer för informationssäkerhet består av detta huvuddokument samt nedan angivna bilagor, vilka utgör en integrerad del av Riktlinjer för informationssäkerhet.

Bilaga 1, Termer och definitioner (i detta dokument)
Bilaga 2, Mall för informationsinventering, klassning, riskbedömning och riskåtgärder (separat bilaga)
Bilaga 3, Skyddsnivåer (separat bilaga)
Bilaga 4, Säkerhetsåtgärder (separat bilaga)

För regler kopplade till Riktlinjer för informationssäkerhet se dokument Regler för Informationssäkerhet

1.3 INTRODUKTION – VAD ÄR INFORMATIONSSÄKERHET?

Information är data som har ett värde för oss och alltså en tillgång som ska skyddas. Informationssäkerhet handlar om att skapa och upprätthålla lämpligt skydd av information. Det innefattar information i alla dess former - muntlig, skriftlig eller digitalt - och oavsett hur information lagras, bearbetas eller kommuniceras. Rätt säkerhet innebär att hantera vår information på rätt sätt.

Informationssäkerhet handlar om att rätt information ska finnas tillgänglig för rätt person i rätt tid. Informationen ska inte kunna förvanskas eller förstöras och den ska inte hamna i orätta händer och missbrukas. I en kommunal verksamhet är spårbarhet en viktig del av informationssäkerheten liksom att det finns tydliga instruktioner kring var informationen lagras och när den eventuellt ska gallras.

För att hålla rätt säkerhet behöver vi struktur, rutiner och skydd av information baserat på fyra aspekter:

Konfidentialitet	att informationen inte tillgängliggörs eller avslöjas för obehörig
Riktighet	att informationen är korrekt, aktuell och fullständig
Tillgänglighet	att informationen är åtkomlig och användbar av behörig
Spårbarhet	att det går att spåra vem som tagit del av eller ändrat informationen

Avvikelser som kan påverka innehållet i någon av dessa aspekter kallas ***incidenter***.

Grundregeln är att allt vi gör inom tjänsten är öppet för insyn och granskning enligt offentlighetsprincipen. Viss information är känslig och måste skyddas från obehöriga att ta del av. Det handlar ofta om hänsyn till den personliga integriteten och för att undvika att enskilda individer kommer till skada.

En stor del av kvaliteten i Höganäs kommuns informationssäkerhet beror därför på hur du som enskild medarbetare hanterar informationen.

1.3.1 INFORMATIONSSÄKERHET OCH DIGITALISERING

I princip alla i samhället – privatpersoner, företag, myndigheter och andra organisationer – använder någon form av digital enhet och allt fler tjänster är beroende av ett gemensamt nätverk - Internet.

När myndigheter, företag och andra organisationer erbjuder digitala tjänster på internet innebär det att informationen inte längre är en organisations ***interna*** tillgång och angelägenhet, utan flödar mellan organisationer i näringsliv och offentlig förvaltning och över nationsgränser. Gränser suddas ut mellan vem som äger och bär ansvar för viss information, vilket gör att det blir svårare att definiera hur den får användas och vem som

kan och får ändra information. Detsamma kan gälla mellan olika verksamheter inom vår organisation.

Utvecklingen innebär utmaningar för en kommuns informationssäkerhet. Information är en viktig och strategisk resurs som genomsyrar alla verksamheter. Utvecklingen där informationshantering och informationsflöden antar nya former, i kombination med en ökad och förändrad hotbild innebär att informationssäkerhet är en förutsättning för att Höganäs kommunkoncern ska kunna delta i det digitala samhället.

2 STYRNING OCH ANSVAR

2.1 ROLLER, ANSVAR OCH ORGANISATION

Ansvaret för informationssäkerheten följer ordinarie verksamhetsansvar. Detta gäller från kommunledningen till den enskilde medarbetaren. Detta innebär att den som är ansvarig för en viss verksamhet också är ansvarig för informationssäkerheten inom verksamhetsområdet.

Kommunen har en informationssäkerhetsansvarig som i samverkan med en utsedd representant (ambassadör) från varje förvaltning / bolag och med informationssäkerhetsrådet stödjer verksamheterna i systematiskt arbete med informationssäkerhet.

2.1.1 ÖVERGRIPANDE ANSVAR

Kommunfullmäktige har ansvar för att fastställa policy, riktlinjer och regler för informationssäkerhet och personuppgiftshantering. Koncernledningen ansvarar för att informationssäkerhetsarbetet bedrivs i linje med den fastställda policyn, med kompletterande riktlinjer och regler och för att alla medarbetare i Höganäs kommun efterlever informationssäkerhetspolicyn. Varje förvaltningschef/bolagschef ansvarar för att förankra dessa riktlinjer och regler i den egna verksamheten.

2.1.2 ANSVAR INOM RESPEKTIVE VERKSAMHET

Varje nämnd och bolagsstyrelse är ansvarig för informationssäkerheten inom sitt verksamhetsområde. Nämnd eller bolagsstyrelse kan vid behov besluta om instruktioner som *kompletterar* de övergripande riktlinjerna för informationssäkerhet. Respektive nämnd/bolagsstyrelse har ett samordningsansvar för informationssäkerheten inom respektive verksamhetsområde. Verksamhetsansvarig, oavsett nivå, ansvarar för informationssäkerheten inom sin verksamhet. Säkerhetsansvaret i sig kan inte delegeras, däremot kan ansvaret att genomföra vissa arbetsuppgifter fördelas.

2.1.3 CHEFS ANSVAR

Varje chef har ett ansvar att delge information och utbildning i informationssäkerhetsfrågor till sina medarbetare samt ge medarbetare förutsättningar att följa de riktlinjer och regler som gäller.

Chefen eller uppdragsgivaren ansvarar för att avgöra om tillgången till känslig information behöver regleras i en tystnads- och sekretessförbindelse. En sådan förbindelse gäller även efter att anställningen eller avtalet upphört.

2.1.4 MEDARBETARES ANSVAR

Alla medarbetare inom verksamheten har ett ansvar för verksamhetens informations-säkerhet.

Om du som medarbetare upptäcker att du har tillgång till som du inte borde ha tillgång till ska du snarast informera din närmsta chef eller uppdragsgivare. Du som medarbetare ansvarar för att

- delta i utbildningar i informationssäkerhet
- i eget arbete följa riktlinjer och regler för informationssäkerhet
- vid användning av IT-stöd ta del av instruktioner om hur dessa resurser ska hanteras, vilka villkor och vilket ansvar som gäller för dessa.
- rapportera informationssäkerhetsrelaterade brister och incidenter.
- vid tillgång till information som du inte borde ha tillgång till ska du snarast informera närmaste chef eller uppdragsgivare.

2.1.5 SYSTEMÄGARES ANSVAR

Systemägare ansvarar för att IT-stöd följer policy för informationssäkerhet- och personuppgiftshantering och de riktlinjer och regler som är kopplade till policyn.

Systemägare är bland annat ansvarig för systemets informationssäkerhet.

Systemägare ska besluta om systemets informationssäkerhetsnivåer genom att klassning sker i enlighet med Höganäs kommuns modell för informationsklassning. Systemägare ska tilldela tillräckligt med resurser i IT-stödets systemförvaltningsplan så att informationssäkerhetsnivån kan uppnås.

Vem som är systemägare ska för varje IT-stöd dokumenteras i en systemförvaltningsplan.

För mer information om systemförvaltning se kommunens systemförvaltningsmodell.

2.1.6 INFORMATIONSÄGARE

En informationsägare är den som har ansvar för en viss informationsmängd. Informationsägaren ska avgöra hur informationen ska klassas och utifrån denna ställa krav på hur information kan och får hanteras och användas. Om ett system har en homogen mängd information som kan kopplas till den verksamhet som en systemägare ansvarar för, är normalt systemägaren även informationsägare. I de fall systemägare inte också är informationsägare för informationen i IT-stöd (till exempel ett diariesystem som hanterar många olika slag av information), så är informationsägare istället kravställare på systemägare vad gäller informationssäkerheten för den aktuella informationen.

2.1.7 PROCESSÄGARE

I större IT-stöd som hanterar flera processer kan det utöver informationsägare även finnas processägare som ansvarar för att processen är ändamålsenlig och effektiv. Processägaren är kravställare på systemägaren i att IT-stödet ska vara ändamålsenligt och effektivt för arbetsprocessen.

2.1.8 SYSTEMFÖRVALTARE

Systemförvaltare ansvarar bland annat för att IT-säkerheten i IT-stöd överensstämmer med verksamhetens krav så att rätt säkerhetsnivå upprätthålls med ett skydd som motiveras av dokumenterad klassning. Systemförvaltare utses av systemägare.

2.1.9 TEKNISK SYSTEMFÖRVALTARE

I en verksamhet ska det finnas en utsedd ägare för aktuella system och som då har ansvaret för säkerheten i systemet. Det ska finnas utsedda ansvariga hos intern eller extern driftsleverantör som kan fungera som motpart till dessa roller så att rätt nivå av säkerhet uppnås. I Höganäs heter den rollen teknisk systemförvaltare.

2.1.10 IT-AVDELNINGENS ANSVAR

IT-avdelningen ansvarar för att säkerheten i kommunens IT-miljö. IT-avdelningen säkerställer att IT-miljön följer verksamhetens krav, legala krav samt policy och riktlinjer för informationssäkerhet och personuppgiftshantering.

2.1.11 IT-SÄKERHETSANSVARIG

IT-chef är IT-säkerhetsansvarig och samordnar arbetet med säkerheten i Höganäs kommuns IT-miljö och är stödjande vid kravställning på externa aktörer.

IT-säkerhetsansvarig ansvarar för kontroll och uppföljning av IT-miljöns IT-säkerhet och omvärldsbevakning inom IT-säkerhetsområdet samt är ytterst ansvarig för säkerheten i IT-miljön.

IT-säkerhetsansvarig är stöd till verksamheter i IT-säkerhetsfrågor, riskanalyser rörande IT-relaterade risker och bistår vid utredningar av misstänkta och inträffade säkerhetsincidenter. Verkar som stöd vid revision och besvarande av revisionsrapporter som berör IT-miljön och dess säkerhet.

2.1.12 INFORMATIONSSÄKERHETSANSVARIG

Informationssäkerhetsarbetet i kommunen leds och samordnas av informationssäkerhetsansvarig. Informationssäkerhetsansvarig ansvarar för att kommunens

övergripande styrdokument är aktuella, att utveckla och förvalta metoder, vägledningar och annat stödmaterial inom informationssäkerhetsområdet (LIS), att i samverkan med ambassadörer för informationssäkerhet stödja verksamheterna i frågor som rör informationssäkerhet och att i samverkan med ambassadörer för informationssäkerhet öka informationssäkerhetsmedvetandet inom kommunen.

Höganäs kommuns IT-samordnare är informationssäkerhetsansvarig.

2.1.13 INFORMATIONSSÄKERHETSAMBASSADÖRER

Varje förvaltning eller bolag utser minst en ambassadör för informationssäkerhet vars ansvar är

- stöd vid informationsinventering, klassning och riskbedömning i den egna verksamheten
- stöd i framtagning och genomförande av handlingsplaner för den egna verksamhetens informationssäkerhet
- tillsammans med informationssäkerhetsansvarig ta fram utbildningsmaterial riktat till den egna verksamheten
- sprida information om övergripande styrdokument kring informationssäkerhet i den egna verksamheten
- att stödja den egna verksamheten i frågor som rör informationssäkerhet,
- öka informationssäkerhetsmedvetandet inom den egna verksamheten

2.1.14 INFORMATIONSSÄKERHETSRÅD

Ett *informationssäkerhetsråd* där kommunens informationssäkerhetsansvarig, IT-säkerhetsansvarig, säkerhetsskyddschef, kris- och beredskapssamordnare, kommunarkivarie samt kommunjurist med dataskyddsansvar ska inrättas och träffas två gånger per år. Informationssäkerhetsrådet leds av kommunens informationssäkerhetsansvarige och rapporterar till koncernledning genom kommunchef. Informationssäkerhetsrådet fungerar som remissinstans och rådgivare i frågor som rör informationssäkerhet och är ett forum för erfarenhetsutbyte och omvärldsbevakning.

2.2 STYRANDE OCH STÖDJANDE DOKUMENT

Följande styrdokument ska finnas som stöd för arbetet med informationssäkerhet.

- **Policy för informationssäkerhet och personuppgifter[3] -** uttrycker ledningens viljeinriktning med informationssäkerhet. Policyn är övergripande, beslutas av Kommunfullmäktige och gäller samtliga förvaltningar och kommunala bolag. Riktar sig till samtliga medarbetare inom Höganäs kommunkoncern.

- R**iktlinjer för informationssäkerhet samt riktlinjer för personuppgifter** - konkretiserar ”Policy för informationssäkerhet och personuppgifter”, innefattar även regler. Beslutas av kommunfullmäktige och gäller samtliga nämnder och kommunala bolag. Riktar sig till alla medarbetare inom Höganäs kommunkoncern.
- **Regler för informationssäkerhet**[4] beslutas av kommunfullmäktige och gäller samtliga nämnder och kommunala bolag. Riktar sig till alla medarbetare inom Höganäs kommunkoncern.
- **Informationsinventering med informationsklassning, riskanalys och riskåtgärder** uppdateras en gång per år i respektive verksamhet samt vid större organisatoriska förändringar eller vid byte av verksamhetssystem. Genomförs i beslutad informationsinventeringsmall – Mall informationsinventering, klassning, riskanalys och åtgärder[5]. Riskåtgärder beslutas av ledningsgrupp i respektive förvaltning / bolag.
- **Handlingsplaner** för informationssäkerhet tas fram av respektive verksamhet årligen och innehåller konkreta mål och åtgärder baserade på informationssäkerhetsanalysen. Beslutas av ledningsgrupp i respektive förvaltning / bolag.
- **Systemförvaltningshandbok**[6] innehåller stöd för verksamheterna att utforma systemförvaltningsplan för respektive IT-stöd. Beslutas av informationssäkerhetsråd och gäller samtliga förvaltningar och kommunala bolag.
- **Utbildningsplan** för informationssäkerhet, personuppgiftshantering och dokumenthantering med koncernövergripande grundutbildning för samtliga medarbetare samt verksamhetsspecifik utbildning för varje verksamhet tas fram av informationssäkerhetsansvarig i samråd med informationssäkerhetsambassadörer.
- **Dokumenthanteringsplan**, som innefattar regler för gallring/bevaring/lagringsplats och informationsklassning för verksamhetens information. Beslutas av respektive nämnd och omfattas av reglerna i arkivreglementet.
- **Systemförvaltningsplan** – varje IT-system ska ha en systemförvaltningsplan som beskriver förvaltning, utveckling, ansvar, behörighetsstruktur för det aktuella systemet. Systemägare ansvarar för att systemförvaltningsplan finns för varje IT-system. Systemförvaltningsplan ska följa framtagen mall enligt systemförvaltningshandbok[7] och ska innehålla information om vilka dokument som ska finnas för varje IT-system och var de förvaras. Se systemförvaltningshandbok för mer information.
- **Informationsklassning av IT-system**- Varje IT-system ska genomgå en klassning av informationssäkerhetsnivå. Systemägare ansvarar för att informationsklassning sker och dokumenteras.

2.3 LEDNINGSSYSTEM FÖR INFORMATIONSSÄKERHET

I Höganäs kommuns informationssäkerhetspolicy anges att vi ska bedriva ett systematiskt informationssäkerhetsarbete med målet att skapa ett ledningssystem för informationssäkerhet (LIS). Systematiskt informationssäkerhetsarbete är att arbeta förebyggande och att kontinuerligt anpassa skyddet utifrån organisationens behov och risker. Då finns informationen tillgänglig när vi behöver den, vi kan lita på att den är riktig och inte manipulerad och att endast behöriga personer får ta del av den. Ett LIS är ett etablerat begrepp för ett systematiskt arbete med informationssäkerhet och innebär en metodik som syftar till att upprätta, införa, driva, övervaka, granska, underhålla och förbättra organisationens informationssäkerhet. LIS avser här inte ett IT-baserat system utan en metodik.

Eftersom kommunen och dess omvärld är i ständig förändring är informations-säkerhetsbehovet dynamiskt och måste ständigt anpassas till exempelvis organisationsförändringar, nya lagar, nya hotbilder och strömningar i samhället. Det räcker därför inte att skapa ett skydd som svarar mot interna och externa förutsättningar idag, eftersom dessa kan se annorlunda ut i morgon. Ett systematiskt arbete med informationssäkerhet med ett LIS syftar i stort till att informationssäkerheten anpassas efter interna och externa förutsättningar, och som därigenom upprätthåller en lämplig skyddsnivå över tid.

Höganäs kommuns LIS bygger på de internationella standarderna för informationssäkerhet i ISO/IEC27000-serien och utgår från metodstöd framtaget av MSB (Myndigheten för samhällsskydd och beredskap).

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

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

2.4 INFORMATIONSKLASSNING

Informationsklassning är en grundläggande komponent i informations-säkerhetsarbetet. Genom att klassa information utifrån krav på dess konfidentialitet, riktighet, tillgänglighet och spårbarhet skapar vi förståelse för, och kan styra vilket skydd som krävs för olika informationsmängder. Klassning av information ska ske utifrån rättsliga krav som lagar och

föreskrifter, men även interna krav på informationens värde, känslighet och betydelse för Höganäs kommuns verksamheter. Idén med informationsklassning är att skydd ska anpassas till kraven på en viss informationsmängd. En viss information kan exempelvis vara mycket kritisk när det gäller tillgänglighet och riktighet, men mindre känslig när det gäller konfidentialitet.

Att klassificera information på ett enhetligt sätt utifrån konfidentialitet, riktighet, spårbarhet och tillgänglighet är en fundamental aktivitet i ett ledningssystem för informationssäkerhet (LIS). En modell definierar nivåer av skyddskrav kopplat till de fyra aspekterna konfidentialitet, riktighet, tillgänglighet och spårbarhet så att information kan klassas på ett enhetligt sätt i hela organisationen.

2.4.1 ORGANISATORISKA SKYDDSÅTGÄRDER

Organisatoriska skyddsåtgärder i ett LIS syftar till att användare och ledning ska ha tillräcklig kunskap om informationssäkerhet och de regler som gäller. Alla medarbetare ska få utbildning i informationssäkerhet och de regler som gäller. En utbildningsplan som omfattar alla medarbetare är framtagen och revideras årligen. Varje förvaltning och bolag genomför en informationsinventering med tillhörande klassning, riskbedömning, riskhantering och handlingsplan för informationssäkerhet i den egna verksamheten. Inventering och handlingsplan uppdateras en gång per år.

2.5 HÖGANÄS MODELL FÖR INFORMATIONSKLASSNING

Höganäs kommun har i och med dessa riktlinjer antagit en egen modell för informationsklassning. Modellen baseras på Sveriges nationella modell för informationsklassning som är utgiven av MSB och SIS, men har anpassats till kommunens behov och dokumenteras i framtagen i bilaga **2**, *mall för informationsinventering, klassning, riskbedömning och riskåtgärder.*

Modellen utgår från de fyra aspekterna konfidentialitet, tillgänglighet, riktighet och spårbarhet och de fyra skyddsnivåerna öppen, grundläggande, utökad och hög. Skyddsnivåerna konkretiseras i skyddsåtgärder för varje nivå för att definiera hur informationen får och ska hanteras.

2.5.1 SKYDDSNIVÅ OCH SKYDDSÅTGÄRDER

Öppen skyddsnivå innebär att det är försumbar påverkan för enskild individ eller för Höganäs kommunkoncern ur aspekterna konfidentialitet och spårbarhet. Öppen information behöver inte ha något skydd mot insyn och har normalt ingen begränsad åtkomst. Däremot är det viktigt att förstå att all information – även öppen – har minst normala skyddskrav när det gäller dess riktighet och tillgänglighet (*). Det kan också krävas

beslut för att viss information ska vara öppen och publik. För öppen nivå finns inga skyddsåtgärder gällande lagring, delning, behörighet, fysisk säkerhet eller distansarbete utöver det som anges i verksamhetens dokumenthanteringsplan.

Grundläggande skyddsnivå gäller för information där påverkan är måttlig. Om informationen innehåller personuppgifter som inte är känsliga gäller grundläggande skyddsnivå. Skyddsåtgärderna i den här nivån omfattas av allmän behörighet, informationen kan kommuniceras och/eller delas internt och externt efter sekretessprövning, informationen får hanteras i mobila enheter och distansarbete är tillåtet.

Utökad skyddsnivå gäller för information där påverkan är betydande. Informationen i den här nivån omfattas av lagstiftning inom kärnverksamhetens område eller specifik generell lagstiftning såsom sekretess enligt OSL, dataskydd enligt GDPR etcetera. Skyddsåtgärderna i den här nivån är särskild behörighet, informationen ska hanteras i anvisade IT-stöd, får delas/kommuniceras internt inom egen verksamhet och externt efter riskbedömning och distansarbete är tillåtet i privat lokal (alltså ej buss, tåg, flyg eller offentligt nätverk) på anvisad enhet efter beslut från verksamhetsansvarig. Informationen får skrivas ut men förvaras inlåst.

Hög skyddsnivå är den högsta nivån och där konsekvenserna är allvarliga för organisationen eller enskild individ. Information som omfattas av specifik lagstiftning såsom NIS-direktivet och lag (2018:1174) om informationssäkerhet för samhällsviktiga och digitala tjänster till skydd för samhällsfunktioner eller känsliga personuppgifter i artikel 9 GDPR, till skydd av enskilda individers rättigheter har hög skyddsnivå. Informationen får enbart hanteras i avsedda IT-stöd, den får endast distribueras enligt listor godkända i dokument eller av informationsägare, särskild behörighet av auktoriserad personal, informationen får inte hanteras i mobila enheter, distansarbete är ej tillåtet utan särskilt beslut av informationsägare och detta ska föregås av dokumenterad riskbedömning.

2.5.2 VAD SKA KLASSIFICERAS?

Det är informationen som är den primära tillgången och som ska klassas. Informationsklassningen styr vilka skyddsåtgärder de olika nivåerna medför. Resurser som används för att hantera informationen, till exempel programvaror, tjänster och fysiska tillgångar, ska utformas och anpassas till de krav som klassningen i förlängningen ställer på dessa. IT-stöd ska klassas på grundval hur informationen är klassad som finns i eller hanteras av systemen. En viktig uppgift för objektägare och systemförvaltare är därför att klassa sina system så att rätt skyddskrav erhålls. Klassning av ett system baseras på klassningen av den information systemet hanterar. Ett system kan lägst ge den klassning som den ingående informationen har. Innehåller systemet en stor mängd information baseras systemklassningen på den information som bedöms som kritisk i systemet.

2.6 DOKUMENTATION AV INFORMATIONSSÄKERHET

Informationssäkerhet ska vara en naturlig del i förvaltningen av objekt och de system som ingår i objekt. Informationsklassningen med tillhörande riskbedömning och riskhantering dokumenteras i inventering som revideras en gång per år enligt dessa riktlinjer. De flesta verksamheter i Höganäs kommunkoncern har behov av ett eller flera verksamhetsspecifika IT-stöd. Samtliga IT-stöd ska ha en systemförvaltningsplan där förvaltning inklusive specifika regler, rutiner och utbildningsinsatser anges. Till stöd för framtagande av denna finns en systemförvaltningshandbok.

2.7 MEDARBETAREN

Medarbetare är den viktigaste resursen i kommunen, och det är medarbetare som dagligen hanterar information, manuellt eller digitalt. Många roller kommer i kontakt med och hanterar kritisk och känslig information, och det är därför att av största vikt att medarbetare får information och utbildning om informationssäkerhet, och att det finns arbetsprocesser i samband med anställning, förändring och avslut av anställning.

2.7.1 FÖRE OCH I SAMBAND MED ANSTÄLLNING

Bakgrundskontroll av sökande till tjänster i Höganäs kommun ska ske genom verifiering av sökandes meritförteckning, till exempel genom kontakt med referenser och bekräftelse av påstådda akademiska och yrkesmässiga kvalifikationer. För vissa kritiska tjänster krävs en förstärkt kontrollform av kreditupplysning och kontroll i brottsregister. Sådana kritiska tjänster är högre chefstjänster, säkerhetstjänster, eller för de som har åtkomst till känslig eller samhällsviktig information. Lagsstiftningen om registerkontroll för skydd av barn och unga ska självklart efterlevas.

För befattningar som har betydelse för rikets säkerhet, och således omfattas av säkerhetsskyddslagen (2018:585) ska det i anställningsförfarandet genomföras en säkerhetsprövning inklusive en registerkontroll. Registerkontrollen ska genomföras innan en person genom anställning eller på annat sätt deltar i verksamhet som har betydelse för rikets säkerhet. De befattningar som är aktuella ska framgå av Höganäs kommuns säkerhetsskyddsplan[8]. Alla bakgrundskontroller ska ta hänsyn till gällande lagstiftning rörande behandling av personuppgifter.

Nyanställda ska delges ansvar och skyldigheter kopplade till informationssäkerhet och genomgå grundläggande utbildning i informationssäkerhet enligt utbildningsplan samt ta del av informationssäkerhet för medarbetare enligt dessa riktlinjer.

Alla anställda (och externt kontrakterade) som får tillgång till konfidentiell information ska underteckna ett sekretessavtal som även ska gälla efter avslut av anställning. Anställande chef eller ansvarig för avtal med externt kontrakterad ansvarar för att informera om innebörd i sekretess och att avtal undertecknas.

2.7.2 UNDER ANSTÄLLNING

Medarbetare inom kommunen ska ha ett högt medvetande avseende informationssäkerhet. Alla medarbetare och i förekommande fall externa aktörer ska en gång per år enligt beslutad utbildningsplan genomgå grundläggande samt verksamhetsspecifik utbildning i informationssäkerhet.

Roller som har särskilda uppgifter inom informationssäkerhet, IT-säkerhet eller systemförvaltningsorganisationen, ska få lämplig fortbildning inom området som är relevant för respektive befattning. Om anställda bryter mot gällande informationssäkerhetsregler ska dessa ärenden hanteras individuellt av ansvarig chef med stöd från HR-avdelningen på samma sätt som vid andra misskötselärenden.

2.7.3 AVSLUT ELLER ÄNDRING AV ANSTÄLLNING

Vid avslut eller ändring av anställning kan ansvar och skyldigheter för informationssäkerhet förbli gällande, exempelvis sekretessavtal och tystnadsplikt om den anställde haft tillgång till konfidentiell information. Detta ska definieras och kommuniceras till den anställde vid anställning/tillträdande av roll och framgå i sekretessavtal. Återlämnande av IT-resurser och indrag av åtkomsträttigheter till information och IT-resurser ska ske i direkt samband med avslut eller ändring av anställning.

2.8 UPPHANDLING AV IT-STÖD

Informationssäkerhetsklassningen ligger till grund för de IT-säkerhetskrav som behöver ställas vid upphandling av IT-stöd. Informationssäkerhetsansvarig tillsammans med IT-säkerhetsansvarig, kommunarkivarie, kommunjurist och upphandlingsenheten ska tas fram kravlista för IT-stöd baserat på kraven i dessa riktlinjer samt interna IT-säkerhetskrav. Denna kravlista ***ska*** bifogas samtliga upphandlingar gällande IT-stöd. Kravlistan revideras en gång per år.

I Höganäs kommunkoncern använder vi företrädesvis upphandlade IT-stöd. Vid användning av appar eller digitala tjänster som inte omfattas av upphandlingskrav ansvarar verksamhetsansvarig för att informationen kan hanteras enligt krav utifrån klassning och att appen/tjänsten uppfyller de krav som finns avseende säkerhetsåtgärder och personuppgiftshantering.

2.9 EFTERLEVNAD OCH GRANSKNING

Efterlevnad av de styrande dokumenten p*olicy för informationssäkerhet och personuppgiftshantering KS/2019/255* och tillhörande riktlinjer ska följas upp. I praktiken innebär det främst uppföljning av att riktlinjerna efterlevs och att säkerhetsåtgärder införs och får avsedd verkan. I synnerhet gäller detta de särskilda säkerhetsåtgärder som gäller för information, objekt och IT-stöd med höga skyddskrav. Granskning och uppföljning av informationssäkerhet, inklusive dess styrning, kommer att utvecklas i och med det ledningssystem för informationssäkerhet (LIS) som ska införas i kommunen då en väsentlig del i ett LIS handlar om efterlevnadskontroll.

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

3 INFORMATIONSSÄKERHET FÖR MEDARBETARE

Detta kapitel vänder sig till alla medarbetare vid Höganäs kommunkoncern.

Riktlinjerna beskriver det ansvar du som medarbetare har vid hantering av information hur informationen ska hanteras. Till dessa riktlinjer finns regler för informationssäkerhet (*Regler för informationssäkerhet KS/2022/100)* som du också ska följa.

Riktlinjer och regler gäller även extern personal som har tillgång till Höganäs kommunkoncerns information, exempelvis uppdragstagare, förtroendevalda eller inhyrda konsulter.

Kompletterande regler och rutiner finns i verksamheten för specifika IT-stöd i systemförvaltningsplan[9] eller i handlingsplan för informationssäkerhet. Informationens klassning (öppen, grundläggande, utökad eller hög) är det som tillsammans med skyddsåtgärderna avgör hur informationen får hanteras.

Du har ansvar för att du hanterar den information du kommer i kontakt med i samband med din anställning/ditt uppdrag korrekt. Här tar vi upp ett par punkter du behöver känna till och följa. Dessa konkretiseras i regler för informationssäkerhet. Det finns i varje verksamhet särskilda regler som du får information om i din verksamhet. Du ansvarar för att följa riktlinjer och regler. Kontakta din chef vid eventuella oklarheter.

3.1 UTBILDNING OCH INFORMATION

Du får vid nyanställning och sedan en gång per år grundläggande utbildning i informationssäkerhet och behandling av personuppgifter samt verksamhetsspecifik utbildning och information om lagringsplats och regler för användning av verksamhetens IT-stöd. Du ansvarar för att ta del av löpande information om informationssäkerhet som delges via intranätet, APT eller andra informationskanaler inom verksamheten.

3.2 INCIDENTER

Alla medarbetare har skyldighet att rapportera incidenter eller brister som misstänkts kunna medföra negativ påverkan på Höganäs kommuns information.

En incident är en avvikelse från normala rutiner. Det kan till exempel vara inbrott, förlust av klientenhet eller information, försök att få tillgång till information med mera. Alla incidenter eller brister ska rapporteras via Höganäs kommuns process för incidentrapportering.

3.3 PERSONUPPGIFTER

En stor del av den information vi hanterar innehåller personuppgifter. För alla medarbetare gäller en skyldighet att behandla personuppgifter enligt bestämmelserna i dataskyddsförordningen (GDPR) och dataskyddslagen (lag (2018:18) med kompletterande bestämmelser till EU:s dataskyddsförordning). Det finns riktlinjer och regler för personuppgiftshantering (R*iktlinjer för personuppgiftshantering KS/2022/10*) som ska följas. Utbildning i behandling av personuppgifter ingår i den utbildningsplan som är framtagen för informationssäkerhet.

3.4 LAGRING OCH SÄKERHETSKOPIERING

Det är viktigt att information lagras på ett säkert sätt och att digital information säkerhetskopieras så att den kan återskapas i händelse av oavsiktlig radering med mera.

Av den anledningen är det viktigt att du som medarbetare alltid förvarar information på anvisad plats eller anvisat system. Var och hur länge information ska bevaras ska framgå av dokumenthanteringsplanen.

3.5 SPÅRBARHET OCH LOGGNING

Spårbarhet innebär att man genom loggning kan identifiera och följa förloppet för olika händelser. Loggning sker i kommunens system, klientenheter och nätverk och innebär att uppgifter om vem som gjorde vad, och när, sparas. Det gäller både de åtgärder som användaren vidtar, samt de åtgärder som systemet vidtar automatiskt när användaren arbetar med klientenhet.

Loggarna används för felsökning och för utredning av incidenter eller för att förhindra brott. Loggarna lagras under en viss tid, och är åtkomliga endast för en begränsad grupp administratörer. All internettrafik och e-post loggas. Manipulation av loggar är ett vanligt sätt att försöka dölja intrång och bedrägeri på.

Höganäs kommun har som arbetsgivare rätt att gå igenom dessa loggar för att kontrollera efterlevnad av lagstiftning, riktlinjer, felsökningar eller vid annan utredning av skada eller hot. Vid misstanke om brott kan loggfilerna komma att lämnas ut till rättskipande myndighet utan att du som kontoinnehavare meddelas.

3.6 SÄKERT BETEENDE

Hur och var vi hanterar information är också en viktig del, vi blir allt mer mobila och det innebär att vi bär information med oss i allt större utsträckning. Telefonsamtal kan höras av andra om du är på en publik plats eller till exempel lämnar ett möte för att besvara ett samtal.

Du ansvarar för att informationen inte oavsiktligt kan läsas eller höras av någon annan när du arbetar i en publik miljö som tåg, flygplats eller utbildningstillfällen. Viss information får du inte hantera i offentliga miljöer.

Informationens klassning avgör hur du får hantera den, information med högt skyddsvärde får inte hanteras utanför kommunens fysiska lokaler utan särskilda beslut. Det innebär att du inte heller kan prata i telefon om, arbeta på distans med eller skriva ut informationen. Du behöver veta vad som gäller för den information du hanterar. Den utbildningen/informationen får du i din verksamhet.

3.7 SKYDD AV UTRUSTNING

Utrustning ska placeras och skyddas för att skyddas mot stöld och miljörelaterade hot som värme, kyla, fuktighet, vätska samt partiklar i luft. Användning ska ske i enlighet med de instruktioner som framtagits av utrustningens ägare. Riskerna för åverkan och stöld är högre i vissa av kommunens egna lokaler, till exempel där många externa personer frekvent vistas och i publika lokaler. Där krävs stöldskydd (till exempel fastlåsning) och märkning. Speciellt utsatt är också mobil utrustning där risken för förlust, stöld och skada är högre. Därför ska mobil utrustning som är avsedd att användas utanför kommunens lokaler förses med stöldskydd och märkning. Användning ska ske i enlighet med de riktlinjer och regler som gäller distansarbete och mobil utrustning där användare till exempel ska säkerställa att utrustning antingen övervakas eller låses in för att minska risken för stöld.

Tänk alltid på hur du hanterar information och vem som kan få del av den.

3.8 ANVÄNDARNAMN OCH LÖSENORD

Ditt användarnamn och lösenord är personligt och förlust av detta kan ge obehörig åtkomst till information som kan vara känslig eller leda till skada för tredje person.

4 INFORMATIONSSÄKERHET I VERKSAMHET

Informationssäkerhet ska vara en naturlig del i alla kommunens verksamheter. Informationsklassningen med tillhörande riskbedömning och riskhantering dokumenteras i inventering som revideras en gång per år enligt dessa riktlinjer. De flesta verksamheter i Höganäs kommunkoncern har utöver de koncernövergripande gemensamma IT-stöden, behov av ett eller flera verksamhetsspecifika IT-stöd. Samtliga IT-stöd ska ha en systemförvaltningsplan där förvaltning inklusive specifika regler, rutiner och utbildningsinsatser anges. Till stöd för framtagande av denna finns en systemförvaltningshandbok. Innehållet följer den vägledning och standard för systematiskt arbete med informationssäkerhet som MSB tagit fram.

4.1 ANSVAR FÖR INFORMATIONSSÄKERHET I VERKSAMHET

Verksamhetsansvarig, oavsett nivå, ansvarar för informationssäkerheten inom sin verksamhet. Det åligger varje verksamhetsansvarig att se till att sina medarbetare efterlever riktlinjer, har ett säkerhetsmedvetande och tillräcklig förståelse och kunskap för att en erforderlig informationssäkerhet i verksamheten kan uppnås. Säkerhetsansvaret i sig kan inte delegeras, däremot kan ansvaret att genomföra vissa arbetsuppgifter fördelas.

Ett par grundregler gäller för alla verksamheter

- All information som hanteras i verksamheten ska finnas angiven i verksamhetens dokumenthanteringsplan.
- Klassificering av informationen sker i angiven mall för informationsinventering, klassning, riskbedömning och riskåtgärder.
- Alla verksamhetsspecifika IT-stöd ska minst ha en utsedd systemägare och systemförvaltare
- För alla verksamhetsspecifika IT-stöd ska en systemförvaltningsplan upprättas och revideras årligen.

Informationsklassningen ligger till grund för systemets klassning och instruktionerna för informationssäkerhet i systemförvaltningsplanen. Det finns en systemförvaltningshandbok framtagen till stöd för upprättande av systemförvaltningsplan.

Av systemförvaltningsplanen ska minst framgå

- Vem som är systemägare, informationsägare och systemförvaltare
- Vilka informationsmängder som hanteras i systemet
- Hur systemet är klassat
- Planerade och genomförda riskanalyser och resultat från dessa
- Hur behörighetshantering och loggning går till
- Hur ändringshantering går till

- Användarinstruktioner med inriktning på säkerhet
- Hur incidenthantering går till
- Vilken kontinuitetshantering som finns

4.1.1 DOKUMENTHANTERINGSPLAN

All information som hanteras i Höganäs kommunkoncern har en bestämd lagringsplats. Lagringsplatsen är anpassad efter informationens skyddsnivå. Eftersom mycket av den information vi hanterar är digital är lagringsplatsen oftast ett IT-stöd. Vilken lagringsplats som gäller framgår av verksamhetens dokumenthanteringsplan. Den är beslutad av respektive nämnd och gäller all information i verksamheten. I dokumenthanteringsplanen anges, förutom lagringsplats, regler för hur informationen ska gallras eller bevaras och om den ska arkiveras. Den innehåller alltså även regler för vilken information du får spara och vilken du ska rensa regelbundet. Du kan i ditt arbete hantera information som ägs av en annan verksamhet, därför kan reglerna även i en annan nämnds dokumenthanteringsplan styra hur du får hantera informationen.

Innehållet och formen för dokumenthanteringsplanen styrs av kommunens arkivreglemente.

4.2 BEHÖRIGHETSHANTERING OCH LOGGNING

Behörigheter innebär vissa rättigheter att använda informationsobjekt, exempelvis ett IT-stöd, på ett specificerat sätt. Behörigheter, eller åtkomsträttigheter, definierar vad en användare har rätt att utföra, till exempel läsa, söka, skriva, radera, skapa eller köra ett program. För att skydda information mot obehörig åtkomst behöver användare ange en identitet som kan verifieras (autentiseras), vanligen med användarnamn och lösenord.

Varje användaridentitet ska vara unik och loggning ska ske för att kunna spåras till en ansvarig person. Gruppidentiteter är inte tillåtna.

4.2.1 BEHÖRIGHETSTILLDELNING

Grundprincipen för behörighet ska baseras på verksamhetens art och dess krav på informationens konfidentialitet och riktighet, tillsammans med legala krav som lagar, föreskrifter och avtal.

Behörighetsroller ska skapas utifrån vilken information användare behöver för att kunna utföra sina arbetsuppgifter. Olika roller som använder ett system kan ha olika behov av information och ska därför ha olika typer av behörigheter eller åtkomstprofiler.

En förutsättning för rätt behörighetstilldelning är att informationen är strukturerad och klassad så att rätt åtkomstregler kan upprättas.

Det ska i systemförvaltningsplanen finnas en process som underhåller och förvaltar behörigheter för ett system, exempelvis hantering av beställning, ändring och borttagning av behörigheter och rättigheter.

Förändringar i användares roller måste återspeglas i behörighetshanteringen, till exempel att användare får andra arbetsuppgifter eller avslutar sin anställning.

Regelbunden uppföljning och revision av samtliga åtkomsträttigheter ska ske kontinuerligt.

4.2.2 ALLMÄN BEHÖRIGHET

Allmän behörighet är grundläggande behörighet till IT-miljön och tilldelas vid anställning, denna kan se olika ut beroende på funktion och uppdragsroll. Den anställde får behörighet till gemensamma system och arbetsytor.

För allmän behörighet finns en process för att säkerställa att reglering av åtkomst sker vid anställning, vid förändring av roll eller arbetsuppgifter samt vid upphörande av anställning.

4.2.3 SÄRSKILD BEHÖRIGHET

Särskild behörighet är all behörighet som inte tilldelas med automatik i samband med anställning. För särskild behörighet är det ansvarig chef i verksamheten som **beslutar** vilka som ska få åtkomst och vilka behörigheter dessa ska ha. Åtkomst gäller alla informationsresurser, inte enbart de som finns i IT-system.

Systemförvaltare **tilldelar** behörigheter i enskilda IT-system.

Behörighetstilldelning följer de förutsättningar som angetts i systemförvaltningsplanen för respektive IT-system. För särskilda administrativa åtkomsträttigheter gäller att de ska vara restriktiva och ge endast de rättigheter som behövs för att utföra sitt uppdrag i den administrativa roll man har tilldelats. Det ska finnas rutiner för att uppdatera och ompröva tilldelade behörigheter för varje informationsresurs.

4.2.4 EXTERNA RESURSER

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

4.2.5 LOGGHANTERING

För att erhålla spårbarhet vid incidenter, identifiera trender och upptäcka avvikelser från legala eller interna regelverk ska kommunens IT-system övervakas och loggas avseende användaraktiviteter, avvikelser, fel och informationssäkerhetshändelser.

Då loggning används ska det finnas processer eller rutiner för dess hantering. Sådana ska innefatta hur loggning går till, hur loggar skyddas mot manipulation och obehörig åtkomst, hur länge de sparas och hur de granskas.

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

4.3 LIVSCYKELHANTERING AV IT-STÖD

Det ska finnas dokumenterad livscykelhantering för varje IT-stöd. Höganäs kommuns livscykelhantering finns beskriven i kommunens systemförvaltningsmodell.

4.3.1 SÄKERHETSKRAV PÅ IT-STÖD

Informationssäkerhetsklassning ska göras i kommunens säkerhetsklassningsverktyg, informeras till och dokumenteras av berörda parter, innan anskaffning av IT-stöd eller förändring av befintligt påbörjas.

4.3.2 SÄKERHETSKRAV VID UPPHANDLING AV IT-STÖD

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

I kravspecifikationer ska alltid tydliga krav på säkerhet formuleras som hämtas från kommunens säkerhetsklassningsverktyg och används vid anbudsutvärdering.

- Upphandling av IT-stöd bör alltid göras i samverkan med ansvarig funktion för upphandling.
- Tekniska krav för kommunens IT-miljö ska bifogas.

4.3.3 SÄKERHET VID SYSTEMUTVECKLING

Processer och rutiner ska finnas för att säkerställa att informationssäkerhet designas och införs under utvecklingscykeln av IT-stöd.

Säkerhet ska vara en integrerad del under hela utvecklingsprocessen.

- Regler för säker utveckling av IT-stöd ska upprättas och tillämpas vid systemutveckling.
- Systemförändringar inom utvecklingscykeln ska följa kommunens systemförvaltningsmodell.
- För systemutvecklings- och integrationsåtgärder bör test- och utvecklingsmiljöer upprättas och skyddas över IT-stödets hela livscykel.

- En säker test- och utvecklingsmiljö bör vara separerad från produktion och inkluderar även människor, processer och teknik.
- Utvecklare ska ha en grundkompetens i programvarusäkerhet och utvecklingsprocesser.

Outsourcad systemutveckling ska kravställas, testas och följas upp för att säkerställa funktionalitet.

4.4 ÄNDRINGSHANTERING

Ändringar i IT-stöd ska ske på ett strukturerat sätt för att säkra IT-stödets säkerhet, funktionalitet och användbarhet och för att minimera antalet fel orsakade av förändringen.

Ändringar i IT-stöd ska ske i samråd med systemägare, systemförvaltare och teknisk systemförvaltare samt dokumenteras i systemförvaltningsplan för respektive IT-system.

Större förändringar ska föregås av en riskanalys och godkännas av systemägaren.

4.5 ANVÄNDARINSTRUKTIONER

Systemägare ansvarar för att det finns användarinstruktioner för samtliga användare till ett IT-stöd. Användare ska utbildas enligt instruktionerna och kontroll ska göras att instruktionerna efterlevs. Instruktionerna ska dokumenteras i systemförvaltingsplan för respektive IT-system.

4.6 RISKANALYS

Risker är tänkbara oönskade händelser som kan inträffa och som kan ha en negativ påverkan på mål. Antingen på mål med själva IT-stöd eller på verksamheters mål. En risk är en kombination av hur sannolikt det är att en händelse inträffar och vilken konsekvens händelsen innebär.

Riskanalysens resultat ska dokumenteras. En riskanalys kan leda till åtgärdsbehov som behöver genomföras omedelbart eller på lite längre sikt och ska då tas med i kommande systemförvaltningsplan.

4.7 INCIDENTHANTERING

Informationssäkerhetsrelaterade incidenter är oönskade händelser som kan, eller skulle kunnat, leda till brister i konfidentialitet, riktighet eller tillgänglighet hos information.

Det ska för varje informationsresurs finnas en process för incidenthantering som beskriver nedan processteg.

- **Förebygga** - förberedande åtgärder utifrån ett organisations- och teknikperspektiv.
- **Identifiera** - behandla insamling samt analys av information och data för avgörande om en incident har inträffat.
- **Begränsa** - behandla isolering och avbrott av pågående attack, minimering av spridning samt insamling av bevis för vidare analys.
- **Återställa** - behandla frågor kring vad som krävs för att få tillbaka system till produktionsnivå samt tillvägagångssätt för att undvika incidenter i framtiden.
- **Erfarenheter** - behandla erfarenheterna från en incident, hur kan verksamheten ta lärdom av erfarenheterna för användning i förberedande syfte.

Informationsägare ansvarar för att incidenter upptäcks, samlas in, hanteras, sammanställs och dokumenteras. Incidenter kan delas in i mindre incidenter och allvarliga incidenter.

Mindre incidenter är till exempel mindre tekniska fel i IT-stöd eller att enstaka användare inte följer instruktioner. Instruktioner och rutiner ska finnas för hur användare ska rapportera mindre incidenter.

Allvarliga incidenter är större störningar som till exempel ett längre avbrott, dataintrång skadlig kod eller allvarlig personuppgiftsincident. En allvarlig incident kräver en utredning där dokumentation ska göras.

Systemförvaltare ska i systemförvaltningsplanen ta fram avbrottsplaner att använda vid större avbrott och som ska innehålla ansvarsförhållanden, kontaktpersoner, eskaleringsvägar till interna och externa aktörer. Här ska samverkan ske med IT-avdelningen.

4.8 KONTINUITETSHANTERING

Kontinuitetshantering innebär att man i en organisation systematiskt arbetar med att skapa en god återhämtningsförmåga för kritiska verksamhetsprocesser och minimera konsekvenserna av störningar, avbrott och katastrofer.

Arbetet innefattar att identifiera kritiska verksamhetsprocesser och dessas beroenden av stöd och resurser som till exempel medarbetare, lokaler och verktyg.

- Nyckelpersonsberoende ska undvikas och i den mån det framkommer att organisationen är beroende av nyckelpersoner ska beroendet åtgärdas.
- Krav på kontinuitet av driften av IT-stöd sker i stora delar genom klassning. **Höga skyddskrav** för tillgänglighet innebär högre krav på säkerhetskopiering och redundans.
- Avbrott kan alltid ske oavsett vilka förebyggande skyddsåtgärder som finns. I dessa fall måste verksamheten ha kontinuitetsplaner och rutiner för att kunna fullfölja sitt åtagande även vid systemavbrott.

- Övning och testning av kontinuitetsplaner ska genomföras och utvärderas regelbundet och identifierade brister samt svagheter åtgärdas med syfte att ständigt förbättra kontinuiteten.
- Kontinuitetsplaner vid avbrott ska finnas tillgängliga för de medarbetare som ingår i aktiviteterna, men samtidigt utgör planerna information med högt skyddsvärde och förvaras skyddat så att de inte blir åtkomliga för obehöriga.

5 INFORMATIONSSÄKERHET I IT-MILJÖN

5.1 INLEDNING

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

5.2 HANTERING AV TILLGÅNGAR

5.2.1 IDENTIFIERING OCH TILLDELNING AV ÄGARE

Samtliga system, programvara och enheter ska vara identifierade och tilldelade en ägare.

5.2.2 CERTIFIERING AV HÅRDVARA

Endast hårdvara certifierad för kommunkoncernens IT-miljö får användas. Certifiering av hårdvara för IT-miljö görs av kommunens IT-avdelning. Hårdvara som ansluts till gästnätverk omfattas ej av certifiering.

5.3 KRYPTERING

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

Behov av kryptering ska baseras på IT-stödets informationsklassning. Vanligen finns behov av kryptering då det föreligger **höga skyddskrav** på konfidentialitet och/eller riktighet.

Krypteringslösningar medför risk för oläsbar data. Därför ska alltid en riskbedömning genomföras.

5.4 FYSISK OCH MILJÖRELATERAD SÄKERHET

Fysisk och miljörelaterad säkerhet avser att förhindra otillåten fysisk åtkomst, skador och störningar. Generellt gäller att informationsklassning ska användas som ett stöd för att utforma det fysiska skyddet som alltid måste utgå från vilken information som hanteras.

5.4.1 SÄKRA UTRYMMEN

Säkra utrymmen med särskilda säkerhetskrav är exempelvis rum som används för servrar, switchar, annan kommunikationsutrustning, kontorsutrymmen där känslig information bearbetas samt arkiv.

- Säkra utrymmen ska utformas så att utrustning inte utsätts för vätskeläckage, korrosiva brand- och släckgaser, damm eller motsvarande.
- Säker elförsörjning genom avbrottsfri reservkraft ska finnas i serverhallar för skydd mot elavbrott och andra störningar.
- VA-dragningar i eller i direkt närhet av säkra utrymmen ska undvikas och risker för vatteninträngning hanteras. Om golvbrunn finns ska åtgärder vidtas för att undvika att vatten kan tränga upp.
- Godkänt brandskydd och brandlarm ska finnas. Släckutrustning ska väljas så att inte onödig skada uppstår vid släckning av brand. Ventilation och andra genomföringar mellan brandceller ska förses med brandspjäll.
- Serverhallar med **höga skyddskrav** ska bevakas och fysisk närvaro ska loggas, till exempel tillträdes- eller videoövervakningsloggar.
- För serverhallar och korskopplingsutrymmen eller likvärdiga säkra utrymmen ska tillträde vara restriktiva och endast ges till de personer som behöver tillträde för att utföra sitt uppdrag.
- Tillträdet till säkra utrymmen ska vara begränsat och regleras minst med hjälp av låssystem med separat nyckelsystem. Nyckel-, kort- och kodinnehav ska vara förtecknade.
- Beslut om vem som ges tillträde att arbeta i säkra utrymmen ska vara dokumenterat.
- Personal som beviljats tillfälligt tillträde till säkra utrymmen ska övervakas under hela besöket.
- Rutiner för att arbeta i säkra utrymmen ska utformas och tillämpas. Roller med ansvar för ett säkert utrymme har också ansvar att ta fram en instruktion för hur arbete i respektive lokal får bedrivas.

5.4.2 UNDERHÅLL, REPARATION OCH AVVECKLING AV HÅRDVARA

Underhåll och reparation kräver åtgärder från extern personal och auktoriserade reparatörer med utbildning på den utrustning som ska hanteras.

Avveckling eller återanvändning ska ske på ett sådant sätt att känslig information inte riskerar att komma i orätta händer.

Det kan ibland vara nödvändigt att vidta särskilda åtgärder, till exempel att känslig information flyttas, raderas eller krypteras före hantering sker av utomstående.

5.5 DRIFTSÄKERHET

5.5.1 DRIFTSRUTINER

Dokumenterade driftsrutiner ska finnas. Dessa ska göras tillgängliga för de användare som behöver dem i sitt arbete.

Förändringar i IT-miljön ska utföras enligt fastställd process. Denna process ska säkerställa att alla ändringar som införs på tjänster, moduler och komponenter i IT-miljön är riskbedömda, planerade, kommunicerade, om möjligt testade och godkända.

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

5.5.2 SKYDD MOT SKADLIG KOD

För att skydda mot skadlig kod ska metoder och rutiner för att förebygga, upptäcka, förhindra samt återställa IT-miljön efter angrepp finnas.

Förutom tekniskt skydd är det viktigt att alla användare av IT-stöd och klientenheter informerar sig om hur de kan minska risken för att drabbas av skadlig kod.

Senaste version av säkerhetsuppdateringar är en viktig komponent för att hålla system och applikationer fria från säkerhetsbrister som kan exploateras.

5.5.3 SÄKERHETSKOPIERING

Säkerhetskopiering av information, program och speglingar av IT-system och IT-miljö är en viktig del av driftsäkerheten för att uppnå både riktighet och tillgänglighet av lagrad information.

Detta ger möjlighet att återställa verksamhetsdata efter uppkomsten av ett fel. I vissa fall är det inte möjligt att återställa all information exempelvis information som tillförts efter senaste säkerhetskopiering.

- Vilka skyddsåtgärder som vidtas ska framgå av systemförvaltningsplan och dokumenthanteringsplan.
- Säkerhetskopior ska lagras geografiskt åtskilt från originalmaterialet för att skydda från fysiska incidenter och katastrofer exempelvis brand och översvämning.
- Säkerhetskopior ska testas regelbundet för att säkerställa att återställning fungerar som avsett.

5.5.4 HANTERING AV TEKNISKA SÅRBARHETER

Tekniska sårbarheter i IT-miljön kan innebära exponering för skadlig kod, dataintrång eller andra sårbarheter.

Det ska finnas rutiner för att upptäcka och informera om tekniska sårbarheter så att lämpliga åtgärder kan vidtas för att behandla de risker som sårbarheter medför.

Installation av IT-stöd som inte är godkända av kommunen kan medföra sårbarheter och incidenter, som exempelvis obehörig åtkomst till information, förlust av riktighet eller överträdelse av immateriella rättigheter.

- Regler för installation av IT-stöd ska finnas.

5.6 KOMMUNIKATIONSSÄKERHET

Kommunikationssäkerhet är skydd som används för datakommunikation i syfte att skydda den information som kommuniceras.

5.6.1 NÄTVERKSSÄKERHET

Nätverk ska hanteras och styras för att skydda information i anslutna system och tillämpningar. Rutiner för hantering och förvaltning av nätverk ska finnas.

- Skyddsåtgärder ska införas för att uppnå säkerhet för information i nätverk och anslutna tjänster utifrån klassningen, dvs. krav på konfidentialitet, riktighet och tillgänglighet.
- Nätverk ska segmenteras för att skilja interna och externa nät från varandra. Nätverk för utvecklings-, test- och produktionsmiljöer kan segmenteras då det är motiverat av säkerhetsskäl eller andra ekonomiska skäl.
- Brandväggar och utrustning för segmentering av nätverk behöver revideras regelbundet.
- Kommunikationstjänster mellan Höganäs kommunkoncern och externa nätverk ska dokumenteras och godkännas av IT-avdelningen innan inkoppling får ske.

5.6.2 INFORMATIONSÖVERFÖRING

Kryptering och signering ska användas när information med **höga skyddskrav** avseende konfidentialitet överförs till annan part.

- Avtal som reglerar säker överföring av verksamhetsinformation mellan Höganäs kommunkoncern och extern part ska upprättas.
- Begränsning av e-post som massutskick ska finnas för att förhindra att kapad mailbox används till att skicka ut stora mängder spam.
- E-post till andra organisationer ska skyddas genom standardiserade säkerhetsfunktioner så som SPF, DKIM för skydd mot otillåtet nyttjande av Höganäs kommuns eller dess bolags e-post domäner.
- Informationsöverföring innehållande skadlig kod, virus eller skräppost ska filtreras och blockeras.

5.7 GRANSKNING OCH KONTROLL

Granskning av säkerhet i IT-stöd och IT-miljö ska ske regelbundet för att kontrollera att inga uppenbara sårbarheter exponeras och att tillräcklig säkerhetsnivå upprätthålls.

Sådan granskning kan till exempel vara skanning av sårbarheter med automatiserade verktyg, penetrationstester eller manuella arbetsprocesser där dokumenterade rutiner för granskningskontroll uppfylls.

- Sårbarheter och brister som upptäcks vid granskningar ska tas upp för åtgärdande i genomförandeplaner, till exempel förvaltningsplaner.
- Akuta sårbarheter och brister ska åtgärdas omedelbart.
- Behov av åtkomst till IT-stöd och data inför granskning eller revision ska avtalas med systemägare.
- Aktiviteter vid granskning eller revision begränsas om möjligt till skrivskyddad åtkomst av program och data.
- Granskning som kan påverka tillgänglighet bör utföras under servicefönster eller vid sådan tidpunkt då påverkan på verksamheten är så liten som möjligt.
- All åtkomst vid granskning eller revision ska övervakas och loggas.

Dessa riktlinjer gäller från 2022-04-12.

BILAGA 1 TERMER OCH DEFINITIONER

TERM	DEFINITION
Användaridentitet	En individuell och unik identitet som används för att skydda information mot obehörig åtkomst och som kan verifieras (Autentisering).
Applikation	Övrig programvara som inte definieras som IT-system.
Autentisering	Verifiering av att en identitet är den som den utger sig för at vara.
Behörighet	Tilldelade rättigheter att använda information eller ett IT-stöd på ett specificerat sätt.
Data	Representation av fakta i form av till exempel tecken eller signaler som är lämpad för överföring, tolkning eller bearbetning av människor eller av automatiska hjälpmedel.
Incident	Avvikelse som kan påverka innehållet i informationen
Höga skyddskrav	Högsta skyddsnivån enligt Höganäs modell för klassificering av information.
Information	Innebörd av data, det vill säga data tolkad av människor.
Informationsklassning	Att genom konsekvensanalys identifiera skyddsbehovet för en viss informationsmängd
Informationssäkerhetsråd	remissinstans och rådgivare i frågor som rör informationssäkerhet och är ett forum för erfarenhetsutbyte och omvärldsbevakning
Informationssäkerhet	Konfidentialitet, riktighet, spårbarhet och tillgänglighet hos information.
Informationsobjekt	Information som är av värde för organisationen, och även de resurser som hanterar den, exempelvis människor, papper, mjukvara, hårdvara och immateriella tillgångar (t. ex. rykte).
Informationsägare	Informationsägare är den som äger och ansvarar för att informationen är riktig och tillförlitlig samt för det sätt informationen sprids.

	Informationsägaren är därmed riskägare för den information som ska hanteras i IT-stöd/lösningen.
IT-infrastruktur	IT-infrastruktur är själva kärnan av IT och utgörs av fysiska och virtuella enheter (som servrar, datorer, nätverk, m.m.).
Kommunkoncern	Samtliga förvaltningar och kommunala bolag i Höganäs kommun
IT-resurs	Personal och/eller budget.
IT-miljö	Kommunens IT-infrastruktur och klientplattform
IT-stöd	IT-system och applikationer.
IT-system	Med IT-system avses ett IT-stöd som samlar in, lagrar, bearbetar och distribuerar information och där igenom stödjer kommunikation inom och mellan organisationerna.
IT-säkerhet	Säkerhet i IT-stöd för att uppnå och upprätthålla informationssäkerhet
Ledningssystem för informationssäkerhet (LIS)	Ett administrativt ledningssystem som syftar till att upprätta, införa, driva, övervaka, granska, underhålla och förbättra organisationens informationssäkerhet.
Policy för informationssäkerhet och personuppgifter	Organisationens viljeinriktning med informationssäkerhet uttryckt av dess ledning.
Processägare	ansvarar för att processen är ändamålsenlig och effektiv
Riktighet	Att information är korrekt, aktuell och fullständig.
Sekretess	Information som inte ska lämnas ut och bli allmänt tillgänglig. Sekretessbelagd uppgift innebär tystnadsplikt för den som har eller fått befattning om uppgiften.

Spårbarhet	Entydig härledning av utförda aktiviteter till en identifierad användare eller IT-stöd.
Tillgänglighet	Att information är åtkomlig och användbar av behörig.
Verksamhetsansvarig	har ansvar för en verksamhet eller del av verksamhet som drivs självständigt och där beslutsmandat finns.

HÄNVISNINGAR

[1] Myndigheter som bedriver säkerhetskänslig verksamhet ska utreda behovet av säkerhetsskydd och dokumentera det i en säkerhetskyddsanalys som svarar på frågorna vad, mot vad och hur ska det skyddas.
[2] Säkerhetsskyddsplan tydliggör vilka säkerhetsskyddsåtgärder som behöver vidtas gällande informationssäkerhet, fysisk säkerhet och personalsäkerhet
[3] Beslutat i ärende KS2015/255 och anger inriktningen för informationssäkerhet och personuppgiftshantering. Finns diarieført i ärende KS2019/255 samt publicerat på intranät.
[4] Separat beslutat dokument med regler som baseras på innehållet i ”Riktlinjer för informationssäkerhet”. Finns diarieført i ärende KS2022/100 samt publicerat på intranät.
[5] Se separat bilaga 2 till dessa riktlinjer ”*Bilaga 2 – Mall för informationsinventering, informationsklassning, riskbedömning och riskhantering*”
[6] Baserat på kommunens riktlinjer för informationssäkerhet finns en systemförvaltningshandbok framtagen för att stödja verksamheterna i arbetet med systemförvaltning. Den finns publicerad på intranät.
[7] Systemförvaltningshandbok, publiceras på intranät
[8] Säkerhetsskyddsplan tydliggör vilka säkerhetsskyddsåtgärder som behöver vidtas gällande informationssäkerhet, fysisk säkerhet och personalsäkerhet.
[9] Systemförvaltningsplan, publiceras på intranät