Informationssäkerhet i byggprojekt

Skapad: 2019-08-26

Senast ändrad: 2021-06-15

locum.
VÄRDEN FÖR VÅRDEN

VI ÄR EN DEL AV REGION STOCKHOLM

Processägare Direktör affärsstöd	Processledare/Uppdateringsansvarig Säkerhetschef	Kvalitetssamordnare Kvalitetschef	Skapat 2019-08-26	Senast ändrat 2021-06-15	Godkänt 2021-06-15

Innehåll

Processägare Direktör affärsstöd	Processledare/Uppdateringsansvarig Säkerhetschef	Kvalitetssamordnare Kvalitetschef	Skapat 2019-08-26	Senast ändrat 2021-06-15	Godkänt 2021-06-15

Informationssäkerhet i byggprojekt

Inledning

Bakgrund

Locum förvaltar, bygger och utvecklar vårdfastigheter åt Region Stockholm. Utöver Locums cirka 300 anställda sysselsätter bolaget flera tusen personer via upphandlade entreprenörer och konsulter. Dessa personer hanterar dagligen stora mängder fastighetsinformation.

Vårdfastigheterna innehåller ett antal system som upprätthåller byggnadernas funktion. Dessa system behöver skyddas mot avsiktliga angrepp och är således skyddsvärda.

Det finns olika sätt att skapa skydd kring Locums skyddsvärden. I stort sätt handlar det om att dels minimera sannolikheten för att ett angrepp ska ske och dels minimera en byggnads sårbarhet mot ett angrepp.

Ett effektivt sätt att minska sannolikheten för angrepp är att begränsa kunskapen om skyddsvärden och var dessa fysiskt finns placerade i fastigheterna. Ingen hotar det som ingen känner till. När kunskapen om värden begränsas minskar möjligheten för en angripare att skaffa sig information om värdena och sannolikheten för ett angrepp minskar.

Felaktigt hanterad information kan således möjliggöra eller underlätta kriminella handlingar eller ge främmande underrättelsetjänst tillgång till uppgifter som kan skada delar av totalförsvaret.

Om skyddsvärd information röjs kan det i förlängningen orsaka skada för Locum och Region Stockholm och kan även vålla fara för Sveriges säkerhet.

Syfte

För att Locum ska kunna förvalta, bygga och utveckla sina fastigheter på ett effektivt sätt, utan att skyddsvärda uppgifter kommer obehöriga till del, är det centralt att personal på alla nivåer i ett projekt kan identifiera och hantera sådana uppgifter.

Syftet med denna anvisning är att ge informationssäkerhetsvägledning vid planering och genomförande av projekt och verksamhet som hanterar Locums fastighetsinformation.

Anvisningen ska säkerställa att Locums informationstillgångar kopplade till vårdfastigheter identifieras, klassificeras och ges en lämplig skyddsnivå med utgångspunkt i att obehöriga inte ska få tillgång till dem (konfidentialitet).

Även övriga informationssäkerhetsaspekter behöver uppfyllas för att projekt ska kunna bedrivas effektivt. Informationstillgångarna behöver alltså också finnas tillgängliga när de behövs (tillgänglighet), vara korrekta (riktighet) samt spårbara (spårbarhet).

Processägare Direktör affärsstöd	Processledare/Uppdateringsansvarig Säkerhetschef	Kvalitetssamordnare Kvalitetschef	Skapat 2019-08-26	Senast ändrat 2021-06-15	Godkänt 2021-06-15

Målgrupp

Målgruppen för denna anvisning är personal som planerar och leder Locums byggprojekt eller som arbetar i Locums förvaltning. Följande typroller är särskilt identifierade:

- Projektområdeschef och projektchef
- Projektledare
- Projekteringsledare, produktionsledare och upphandlare
- Slutsamordnare
- Förvaltningspersonal

Regelverk för informationssäkerheten

Informationssäkerheten regleras från lagar ner till Locums styrdokument i form av policys, riktlinjer, anvisningar och instruktioner. Nedanstående bild visar förhållandena mellan regelverken och var i hierarkin denna anvisning och relaterade dokument befinner sig.

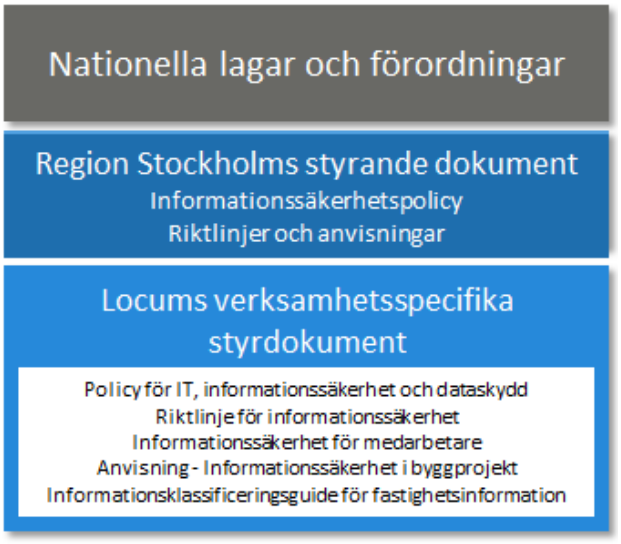


Illustration: Regelverk för informationssäkerheten och förhållandena mellan dessa.

Kort om allmänna handlingar

Enkelt kan man säga att en allmän handling är information i olika former (pappersdokument, ritningar, datafiler, foton etc.) som förvaras hos, inkommit till eller upprättats av Region Stockholm.

Allmänheten har rätt att ta del av Region Stockholms allmänna handlingar om dessa inte omfattas av sekretess enligt offentlighets- och sekretesslagen. Utlämningsärenden av detta slag hanteras enligt särskilda rutiner. Minnesanteckningar, privata brev samt icke justerade protokoll, beslut eller skrivelser faller utanför begreppet allmän handling. Dessa har allmänheten inte rätt att ta del av.

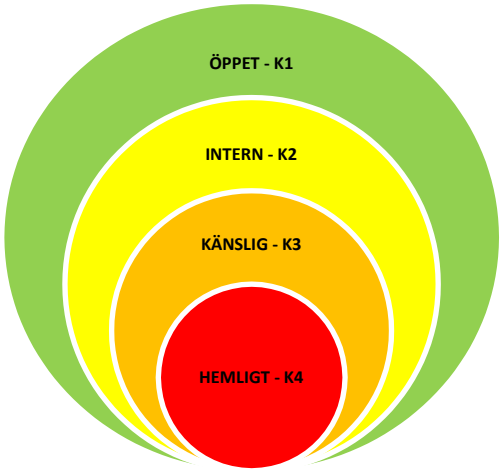
Processägare Direktör affärsstöd	Processledare/Uppdateringsansvarig Säkerhetschef	Kvalitetssamordnare Kvalitetschef	Skapat 2019-08-26	Senast ändrat 2021-06-15	Godkänt 2021-06-15

Locums informationssäkerhetsklasser och krav på hantering

De flesta uppgifter rörande Locums fastigheter är inte uppgifter som omfattas av sekretess. Dessa uppgifter är och benämns som öppna (K1). Allmänheten har rätt att ta del av Region Stockholms öppna allmänna handlingar.

En del av den totala informationen omfattas dock av bestämmelser i offentlighets- och sekretesslagen, så kallade sekretessbelagda uppgifter (K3-Känsliga). Sekretessen medför begränsning i allmänhetens rätt att ta del av allmänna handlingar.

Sekretessen innebär också att uppgifterna ska hanteras och förvaras enligt särskilda bestämmelser.



Illustrationen ovan: Åskådliggör informationssäkerhetsklasser.

En särskild typ av de sekretessbelagda uppgifterna är uppgifter som rör Sveriges säkerhet. De uppgifterna definieras i säkerhetsskyddsförordningen som hemliga uppgifter (K4). För att ta del av hemliga uppgifter krävs särskild prövning och utbildning samt ett behov av uppgifterna för att kunna utföra sitt arbete. Locum använder därför fyra informationssäkerhetsklasser vad gäller informationens konfidentialitet:

1. Öppen (K1)
2. Intern arbetshandling (K2)
3. Känslig (Enligt OSL 18 kap) (K3)
4. Hemlig (Enligt OSL 15 kap 2§) (K4)

Krav på hantering av sekretessklassificerade och hemliga uppgifter återfinns i Locums dokument *Informationssäkerhet - Vägledning för medarbetare*.

Processägare Direktör affärsstöd	Processledare/Uppdateringsansvarig Säkerhetschef	Kvalitetssamordnare Kvalitetschef	Skapat 2019-08-26	Senast ändrat 2021-06-15	Godkänt 2021-06-15

Projektsäkerhet

Allmänt

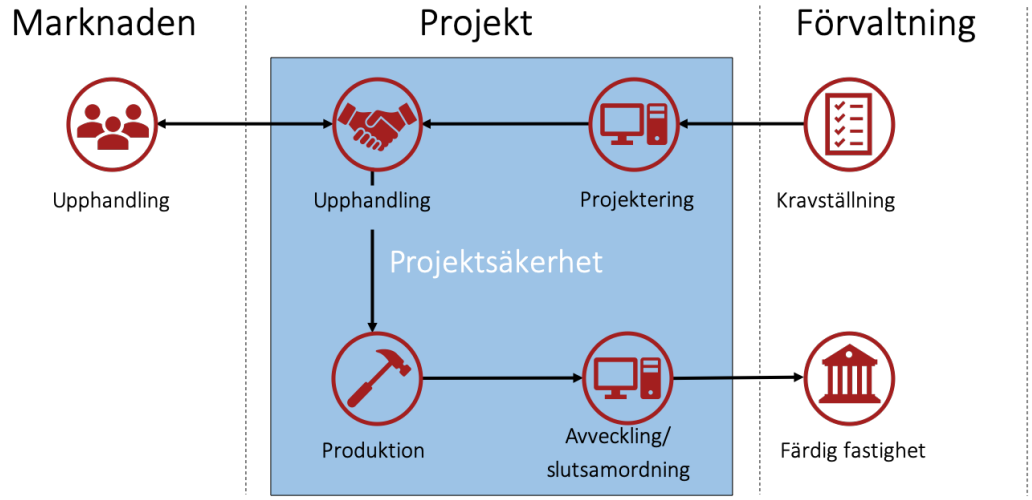
Projektsäkerhet omfattar de tillfälliga säkerhetsåtgärder i ett projekt som syftar till att förhindra att information röjs, förstörs eller förvanskas. Åtgärderna ska också bidra till att skyddsvärd information inom projektet ägs och kontrolleras av Locum.

Syftet med projektsäkerhetsarbetet är att Locums skyddsvärda information ska ha samma nivå av skydd oavsett i vilken fas projektet befinner sig i. Projektsäkerhetsarbetet ska alltså bedrivas under projektets samtliga faser såsom projektering, upphandling, produktion och avveckling/slutsamordning.

Den skyddsvärda informationen i ett projekt ska också skyddas likvärdigt oavsett i vilken form den förekommer. Det spelar alltså ingen roll om uppgifterna framgår av en ritning eller beskrivning, om uppgifterna hanteras inom ramen för en upphandling, om uppgifter hanteras på byggarbetsplatsen eller om uppgifterna framgår i den färdigställda fastigheten.

Projektsäkerhetsåtgärder och ansvarsförhållanden beträffande informationssäkerheten behöver således vara implementerade i samband med att skyddsvärd information börjar hanteras, i praktiken redan i samband med förstudien.

Nedanstående bild beskriver projektsäkerheten i ett projekt från inledande kravställning till färdig fastighet.

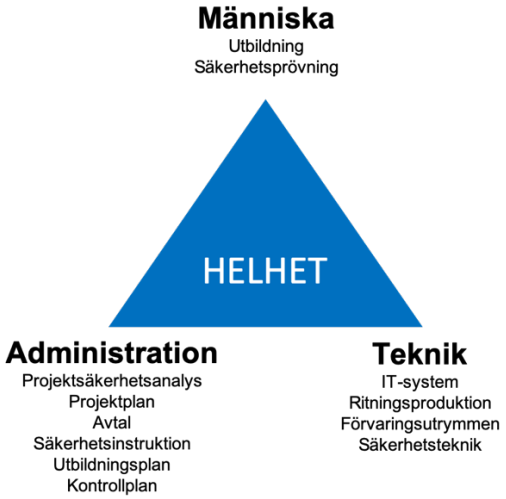


Illustrationen ovan: Principbild utvisande projektsäkerhetsarbete – informationen har samma skydd oavsett projektfas.

Processägare Direktör affärsstöd	Processledare/Uppdateringsansvarig Säkerhetschef	Kvalitetssamordnare Kvalitetschef	Skapat 2019-08-26	Senast ändrat 2021-06-15	Godkänt 2021-06-15

Informationssäkerheten i ett projekt består av olika delar där människa, teknik och administrativa regelverk skapar en helhet. Denna helhet ska således vara anpassad efter projektets natur och de uppgifter och informationssäkerhetsklasser som projektet har att hantera.

Projektet behöver således avvägda resurser i form av personal och andra tillgångar för hantering av sekretessklassificerade uppgifter i alla projektskeden. Dessa tillgångar ska identifieras under projektplaneringen.



Illustrationen ovan: Projektet behöver avvägda resurser i form av personal och andra tillgångar för hantering av sekretessklassificerade uppgifter i alla projektskeden. Dessa tillgångar ska identifieras under projektplaneringen.

Övergripande informationssäkerhetsåtgärder i respektive projektfas

Förberedelser
Övergripande informationssäkerhetsåtgärder som bör genomförs innan projektet startas:

- Informationsklassificera fastighetsinformation enligt Informationsklassificeringsguide för fastighetsinformation
- Upprätta en projektsäkerhetsanalys
- Upprätta säkerhetsinstruktion, utbildningsplan samt kontrollplan för projektsäkerhetsarbetet
- Tydliggör informationsägarförhållanden mot konsulter och entreprenörer
- Identifiera vilka befattningar som eventuellt ska placeras i säkerhetsklass
- Kravställ och/eller upprätta IT-system för hantering av aktuella informationssäkerhetsklasser
- Kravställ och upprätta förvaringsutrymmen som möjliggöra hantering av aktuella informationssäkerhetsklasser

Processägare Direktör affärsstöd	Processledare/Uppdateringsansvarig Säkerhetschef	Kvalitetssamordnare Kvalitetschef	Skapat 2019-08-26	Senast ändrat 2021-06-15	Godkänt 2021-06-15

Projektering
Övergripande informationssäkerhetsåtgärder som bör genomföras under projekteringen:

- Upprätta eventuella sekretess- och säkerhetsskyddsavtal
- Genomför säkerhetsutbildning med aktuella konsulter
- Säkerställ att ritningar och beskrivningar är projekterade så att upphandling kan genomföras utan att röja skyddsvärden.

Upphandling
Övergripande informationssäkerhetsåtgärder som bör genomföras under upphandlingar:

- Upprätta eventuella sekretess- och säkerhetsskyddsavtal
- Genomför säkerhetsutbildning med anbudsgivare
- Kravställ informationsägarförhållanden och informationssäkerhetsåtgärder i avtal gentemot konsulter, leverantörer, entreprenörer mm
- Identifiera om behov föreligger av säkerhetsskyddade upphandlingar.

Produktion
Produktionen präglas av att mycket personal ansluter till- och lämnar projektet. Under detta skede krävs en fungerande behörighetsadministration för att tillmötesgå de informationssäkerhetskrav som ställts.

Goda förutsättningar för informationssäkerhetsarbetet under produktionsfasen skapas genom:

- En effektiv behörighetsadministration
- Utbildning, uppföljning och kontroll av informationssäkerheten
- Fysiskt skydd och teknisk bevakning av skyddsvärden på byggarbetsplatsen
- Säker distribution av bygginformation (fysiska ritningar eller digital hantering)
- Spårbarhet och förvaring av ritningar, läsplattor och beskrivningar
- Eventuella fotoförbud kopplade till projektets skyddsvärden.

Slutskede och förvaltning
Under detta skede sker slutsamordning och överlämning till Locums förvaltning. Följande bör särskilt beaktas i skedet:

- Sluthantering av informationsägarskap gentemot entreprenörer, konsulter, leverantörer mm
- Säkerställ förvaltningens möjlighet till mottagande av projektets skyddade informationstillgångar.

Planering av projektsäkerhet

För att informationssäkerheten ska hålla en jämn nivå är det av väsentlig betydelse att informationen hanteras på rätt sätt.

Processägare Direktör affärsstöd	Processledare/Uppdateringsansvarig Säkerhetschef	Kvalitetssamordnare Kvalitetschef	Skapat 2019-08-26	Senast ändrat 2021-06-15	Godkänt 2021-06-15

För att skapa rätt förutsättningar för informationshanteringen behöver Locums projekt planeras och resurs sättas utifrån informationssäkerhetssynpunkt. Detta görs genom att projektplanen[1] hämtar ingångsvärden från:

- Säkerhetsplanen[2]
- Informationsklassificeringsguide för fastighetsinformation
- Projektsäkerhetsanalysen[3].

Illustrationen ovan: Exempel på planering av projektsäkerhet

Säkerhetsplan

Som grund för säkerhetsarbetet ligger sjukhusets säkerhetsplan som beskriver övergripande grundläggande byggnadstekniska och säkerhetstekniska krav för fastigheten. Säkerhetsplanen förankras och godkänns i samråd mellan Locums säkerhetschef samt eventuell lokal säkerhetschef inom sjukhusområdet.

När säkerhetsplanen är godkänd upprättar projektörer handlingar utifrån upprättad säkerhetsplan och Locums projekteringsanvisningar för teletekniska säkerhetssystem.

Behörighet att ta del av säkerhetsplan inklusive arbetsmaterial regleras av säkerhetschef och aktuell projektledare. Säkerhetsplanen är sekretessbelagd.

Klassificering av fastighetsinformation

Vid hantering av fastighetsinformation, som är av betydelse för att upprätthålla byggnaders funktion, är det viktigt att bedöma om det förekommer uppgifter som behöver skyddas mot obehörig åtkomst. Ett röjande av vissa uppgifter skulle kunna möjliggöra eller underlätta antagonistiska (aktörsdrivna) handlingar mot fastigheter eller mot verksamhet som bedrivs i dessa.

För detta ändamål har Locum en informationsklassificeringsguide som indikerar vilken fastighetsinformation som behöver skyddas. Guiden är vägledande för vilken skyddsnivå som

[1] Se Locums Handbok Byggprojektledning.
[2] Se Locums Projekteringsanvisningar för teletekniska säkerhetssystem, www.locum.se.
[3] Se punkten 4.3

Processägare Direktör affärsstöd	Processledare/Uppdateringsansvarig Säkerhetschef	Kvalitetssamordnare Kvalitetschef	Skapat 2019-08-26	Senast ändrat 2021-06-15	Godkänt 2021-06-15

uppgifterna ska ha och således vilken typ av informationssäkerhetsåtgärder som blir aktuella under projektets faser.

Informationsklassificering ska göras av all fastighetsinformation som hanteras i projektet i syfte att kunna hantera denna med rätt skyddsnivå. Klassificeringen ligger sedan till grund för *projektsäkerhetsanalysen* och *projektplanen*.

För klassificering av byggnadsinformation se dokumentet *Informationsklassificeringsguide för fastighetsinformation.*

Projektsäkerhetsanalys

En projektsäkerhetsanalys ska genomföras för att identifiera de skyddsvärden och de risker som finns inom projektet.

Analysen tillsammans med säkerhetsplanen utgör grunden för de informationssäkerhetsåtgärder som projektet har att prioritera och hantera för att reducera de identifierade skyddsvärdenas sårbarheter.

Projektsäkerhetsanalysen ska:

- Identifiera skyddsvärda informationstillgångar inom projektet
- Bedöma säkerhetshot
- Bedöma respektive informationstillgångs sårbarhet
- Bedöma informationssäkerhetsrisker
- Prioritera och hantera dessa risker

Projektsäkerhetsanalysen tas fram av aktuell projektledare. Den dokumenteras, förankras och godkänns i samråd mellan Locums säkerhetschef samt aktuell projektområdeschef.

Resultatet av analysen ska slutligen inarbetas i projektplanen.

Projektplan

Projektplanen säkerställer att samtliga i projektet jobbar på ett enhetligt sätt och underlättar för nya projektmedlemmar att snabbt få en överblick över projektet. Projektledaren ansvarar för att projektplanen godkänns och efterlevs.

Projektplanen ska därför hämta ingångsvärden från säkerhetsplanen, informations-klassificeringsguiden för fastighetsinformation samt projektsäkerhetsanalysen.

Säkerhetsansvar och roller

Nedanstående bild illustrerar principer och exempel på ansvarsfördelning gällande det säkerhetsarbete som bedrivs inom ramen för ett byggprojekt.

Processägare Direktör affärsstöd	Processledare/Uppdateringsansvarig Säkerhetschef	Kvalitetssamordnare Kvalitetschef	Skapat 2019-08-26	Senast ändrat 2021-06-15	Godkänt 2021-06-15

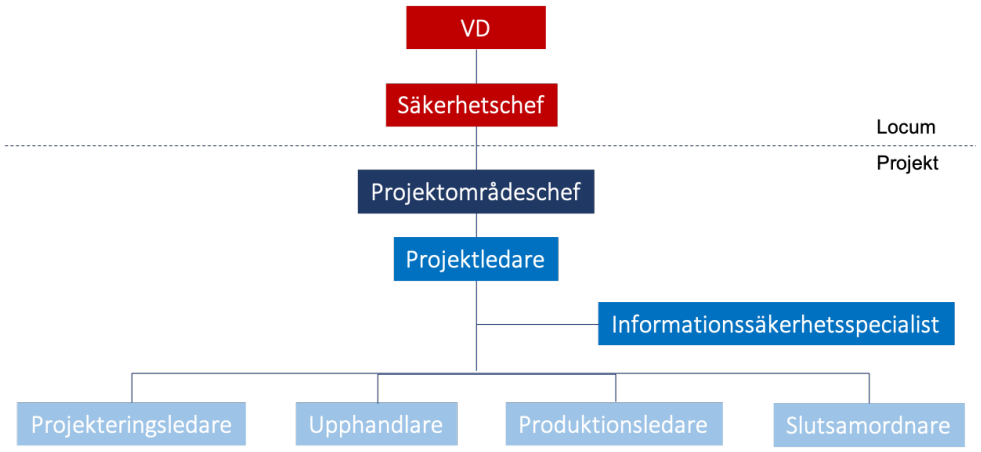


Illustration ovan: Principbild över ansvarsfördelningen i ett byggprojekt. Säkerhetsarbetet är en integrerad del i projektet.

Verkställande direktör

- Är övergripande ansvarig för informationssäkerheten och säkerhetsskyddet inom Locum.

Säkerhetschef

- Är direkt underställd Vd avseende informationssäkerhets- och säkerhetsskyddsfrågor.
- Samordnar, följer upp och kontrollerar projektets säkerhets- och säkerhetsskyddsarbete.
- Ansvarar för beslut om inplacering i säkerhetsklass i projektet.

Projektområdeschef

- Kvalitetssäkrar informationssäkerhetsarbetet.
- Fastställer rutin för sekretess- och eventuella säkerhetsskyddsavtal.

Projektledare

- Har övergripande ansvar för säkerheten under projektets samtliga skeden vad avser säkerhetsskydd, informationssäkerhet (inklusive IT-säkerhet) samt fysisk säkerhet.
- Ansvarar för kravställning av vilka säkerhetsåtgärder som ska vidtas för att skydda informationen under projektets samtliga faser. Ansvarar för att inom projektet upprätta:
  - Säkerhetsplan

Processägare Direktör affärsstöd	Processledare/Uppdateringsansvarig Säkerhetschef	Kvalitetssamordnare Kvalitetschef	Skapat 2019-08-26	Senast ändrat 2021-06-15	Godkänt 2021-06-15

- Projektsäkerhetsanalys
- Säkerhetsinstruktion, utbildningsplan och kontrollplan för projektsäkerhetsarbetet
- Eventuella sekretess- och säkerhetskyddsavtal

Informationssäkerhetsspecialist

Projektets storlek är dimensionerande för hur många informationssäkerhetsspecialister projektet är i behov av.

- Är funktionsansvarig för projektsäkerheten och leder därmed det operativa säkerhetsarbetet i projektet
- Upprättar och underhåller projektets:
  - Säkerhetsplan
  - Projektsäkerhetsanalys
  - Säkerhetsinstruktion, utbildningsplan och kontrollplan för projektsäkerhetsarbetet
- Tillser att informations- och IT-säkerhetsarbetet i projektet följer gällande bestämmelser genom:
  - Utbildning
  - Rådgivning
  - Uppföljning och kontroll
- Ansvarar över samtlig personal som ingår eller har ingått i projektet vad gäller:
  - Behörighet och behörighetsnivåer vad avser information
  - Eventuella säkerhetsprövningar
  - Sekretessbevis
- Ansvarar för det eventuella fysiska skyddet av projektkontor och byggarbetsplats
- Ansvarar för incidenthantering samt vidarerapportering av denna information till projektledare och Locums säkerhetschef

Projektledare

- Koordinerar informationssäkerhetsarbetet under projekteringen och under produktion.
- Ansvarar för vidarerapportering av säkerhetsincidenter till informationssäkerhetsspecialisten.
- Ansvarar med stöd av informationssäkerhetsspecialisten, överlämningen av projektets informationsklassificerade uppgifter till Locums förvaltning.

Processägare Direktör affärsstöd	Processledare/Uppdateringsansvarig Säkerhetschef	Kvalitetssamordnare Kvalitetschef	Skapat 2019-08-26	Senast ändrat 2021-06-15	Godkänt 2021-06-15

Upphandlare

- Koordinerar informationssäkerhetsarbetet under upphandlingar.
- Upprättar sekretess- och/eller säkerhetsskyddsavtal i samråd med informationssäkerhetsspecialisten.
- Ansvarar för vidarerapportering av säkerhetsincidenter till informationssäkerhetsspecialisten.

Säkerhetsskydd och säkerhetsskyddsklassificerade uppgifter

Säkerhetsskydd handlar om att skydda den information och de verksamheter som är av betydelse för Sveriges säkerhet mot spionerі, sabotage, terroristbrott och vissa andra hot.

Säkerhetsskyddet handlar om att genom förebyggande arbete skydda bland annat uppgifter som rör säkerhetskänslig verksamhet och därför omfattas av sekretess enligt offentlighets- och sekretesslagen. De kallas säkerhetsskyddsklassificerade uppgifter och delas in i fyra säkerhetsskyddsklasser, utifrån vilken skada för Sveriges säkerhet som kan uppstå om de röjs:

1. Kvalificerat hemlig
2. Hemlig
3. Konfidentiell
4. Begränsat hemlig

De fyra säkerhetsskyddsklasserna ingår idag i Locum informationssäkerhetsklass K4 (hemlig). Därav delas K4 in i fyra underklasser. De säkerhetsskyddåtgärder som blir aktuella för de olika klasserna skiljer sig åt. Kvalificerat hemliga uppgifter omgärdas av ett högre skydd än begränsat hemliga uppgifter.

Locums säkerhetschef ansvarar för att ange om ett projekt har att hantera säkerhetsskydds-klassificerade uppgifter och vilka uppgifter som i sådana fall är hemliga samt vilken underklass de tillhör.

Avtal beträffande informationssäkerheten

Sekretessavtal

Syftet med ett sekretessavtal är att Locums sekretessbelagda uppgifter ska ha samma skydd hos anlitade företag som de har hos Locum.

Sekretessavtal ska upprättas mellan Locum och anlitade företag om företaget kommer att hantera information eller ges tillgång till säkerhetskänslig verksamhet som informations-säkerhetsmässigt ingår i informationssäkerhetsklasserna K2 och K3. I sekretessavtalet ska förutom regler och villkor för informationshanteringen även anges vem som är informations-ägare till aktuell information.

Rutin för träffande och avslut av sekretessavtal upprättas av informationssäkerhetsspecialisten och fastställs av projektområdeschefen.

Processägare Direktör affärsstöd	Processledare/Uppdateringsansvarig Säkerhetschef	Kvalitetssamordnare Kvalitetschef	Skapat 2019-08-26	Senast ändrat 2021-06-15	Godkänt 2021-06-15

Säkerhetsskyddsavtal

Syftet med ett säkerhetsskyddsavtal är att Locums säkerhetsskyddsklassificerade (K4)[4] uppgifter ska ha samma säkerhetsskydd hos anlitade företag som hos Locum. Säkerhetsskyddslagen ställer krav på att Locum upprättar säkerhetsskyddsavtal vid upphandling om:

- det i upphandlingen förekommer säkerhetsskyddsklassificerade uppgifter i säkerhetskyddsklassen konfidentiellt eller högre[5], eller
- upphandlingen i övrigt avser eller ger leverantören tillgång till säkerhetskänslig verksamhet av motsvarande betydelse för Sveriges säkerhet.

Rutin för träffande och avslut av säkerhetsskyddsavtal upprättas av informations-säkerhetsspecialisten och fastställs av Locums säkerhetsskyddschef.

Personalsäkerhet

Säkerhetsmedvetande

Oavsett vilka skyddsåtgärder som vidtas inom projektet är den enskilde individens säkerhetsmedvetande avgörande för att säkerhetsarbetet ska fungera.

Enskilds säkerhetsmedvetenhet är avgörande för att bevara projektets skyddsvärden.

Projektet ska genom *utbildning och kultur* medvetandegöra de åtgärder som enskild kan göra för att stärka säkerheten inom projektet. Därigenom skapas förutsättningar för att skydda projektets skyddsvärden.

Åtgärderna för att stärka skyddet kan vara att:

- personalen inte lånar ut passerkort, nycklar och koder till någon annan
- tillse att hanteringen av sekretessbelagda handlingar sker på ett korrekt sätt
- kontrollera besökare eller okända personer inom projektet
- tillse att obehöriga och besökare inte kan ta del av sekretessbelagda uppgifter.

[4] Se punkten Säkerhetsskydd och säkerhetsskyddsklassificerade uppgifter.
[5] Se punkten Säkerhetsskydd och säkerhetsskyddsklassificerade uppgifter.

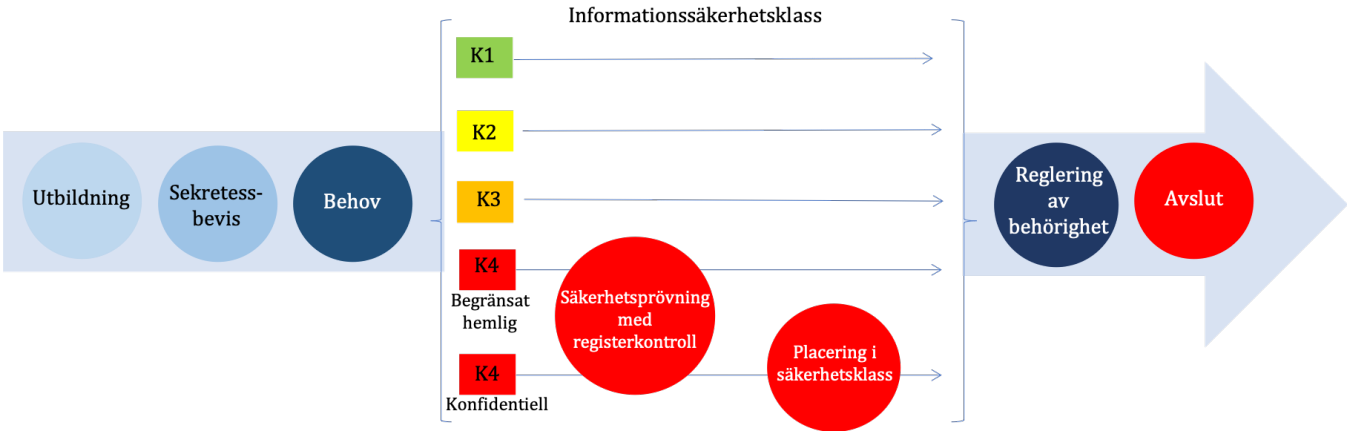
Processägare Direktör affärsstöd	Processledare/Uppdateringsansvarig Säkerhetschef	Kvalitetssamordnare Kvalitetschef	Skapat 2019-08-26	Senast ändrat 2021-06-15	Godkänt 2021-06-15

Behörighetsadministration

Genom en fungerande behörighetsadministration får personal endast tillgång till sådan information som behovs för att kunna utföra sina arbetsuppgifter. Skyddsvärda uppgifter hålls således i en mindre krets och får mindre spridning.

Vilka krav som ställs för att en person ska kunna anses vara behörig till en viss typ av information styrs ytterst av informationssäkerhetsklassen.

Nedanstående bild ger exempel på en process för behörighetsadministration kopplad till informationssäkerhetsklasserna. Processtegen beskrivs närmare nedan.



Illustrationen ovan: Exempel på process för behörighetsadministration.

Utbildning

Alla som tar del av projektet ska genomgå en grundläggande utbildning i informationssäkerhet. Genom utbildningen skapas grundförutsättningar för att informationssäkerhetsarbetet i projektet får avsedd effekt.

Syftet med utbildningen ska vara att höja säkerhetsmedvetandet och klargöra varför och hur man vidtar olika skyddsåtgärder.

Sekretessbevis

Sekretess innebär förbud mot att röja en uppgift vare sig det sker muntligen eller på annat sätt. Denna tystnadsplikt kvarstår även efter det att projektet har upphört.

Den som tillåts att ta del av sekretessbelagda och/eller hemliga uppgifter ska upplysas om omfattningen och innebörden av sekretessen. Samtliga som ska ingå i projektet ska skriva under ett sekretessbevis *innan* vederbörande påbörjar sitt arbete. Sekretessbevis tecknas med fördel i samband med utbildningen.

Behov

Det ska göras en värdering av vilken information och vilken informationssäkerhetsklass personen ska få tillgång till. Denna bedömning ska utgå ifrån om personen:

- Behöver uppgifterna eller annan tillgång till verksamheten för att kunna utföra sitt arbete
- På annat sätt deltar i verksamheten där personen kan exponeras för sekretessbelagd eller/och hemliga uppgifter, t ex städpersonal.

Säkerhetsprövning och inplacering i säkerhetsklass

Säkerhetsprövning ska göras innan personen deltar i säkerhetskänslig verksamhet som bedöms som begränsad hemlig eller högre enligt säkerhetsskyddslagen[6]. Detta kräver god framförhållning då en säkerhetsprövning är tidskrävande.

Inledningsvis ska en grundutredning göras beträffande personen i fråga. Denna ska dokumenteras och innehålla ett personligt samtal där lojalitet, pålitlighet och sårbarhet hos den som prövas ska bedömas. Under projektets gång ska pålitligheten fortlöpande bedömas.

Säkerhetsprövningen ska förutom grundutredningen innefatta en registerkontroll, om befattningen är inplacerad i säkerhetsklass. En registerkontroll kräver aktuell persons samtycke.

Om projektet genomför säkerhetskänslig verksamhet enligt säkerhetsskyddslagen ska personen placeras i säkerhetsklass 3 om vederbörande:

1. Får ta del av uppgifter i säkerhetsskyddsklass *konfidentiell*
2. I ringa omfattning får del av uppgifter i säkerhetsklassen hemlig, eller
3. Till följd av sitt deltagande i verksamheten har möjlighet att orsaka en inte obetydlig skada för Sveriges säkerhet.

De personer som i grund ska placeras i säkerhetsklass 3 i ett projekt är:

1. Projektområdeschef
2. Projektledare
3. Informationssäkerhetsspecialist

Locums säkerhetschef ansvarar för att ange om ett projekt har att hantera säkerhetsskyddsklassificerade uppgifter samt tar beslut om inplacering i säkerhetsklass.

Reglering av behörighet

Den avslutande delen i behörighetsadministrationen innefattar en reglering i vad personen ska få tillgång till. Regleringen innefattar tillträde till byggnader, utrymmen (kort, kod, nycklar) samt behörigheter till IT-system och filareor.

[6] Se punkten Säkerhetsskydd och säkerhetsskyddsklassificerade uppgifter.

Processägare Direktör affärsstöd	Processledare/Uppdateringsansvarig Säkerhetschef	Kvalitetssamordnare Kvalitetschef	Skapat 2019-08-26	Senast ändrat 2021-06-15	Godkänt 2021-06-15

Avslut

Då en person slutar i projektet ska följande beaktas:

- Återlämning av sekretessbelagda och/eller hemliga handlingar
- Personen ska påminnas om innebörden av sekretessen
- Behörigheter till utrymmen och IT-system ska avslutas
- Om personen är registerkontrollerad ska avanmälan ske till säkerhetspolisen.

Fysiskt skydd och tillträdeskontroll

Projektarbete genomförs normalt i kontorslokaler och på byggarbetsplats som, beroende på vilken information som hanteras, kräver olika grader av fysiskt skydd. Det fysiska skyddet ska hindra obehörigt tillträde till område eller yta där skyddsvärd information hanteras eller förvaras.

Det fysiska skyddet kan delas in i flera lager för att hantera olika typer av hot som kan påverka informationen. Det skyddsåtgärder som kan vara aktuella är:

- Perimeterskydd (områdesskydd) såsom staket och grindar
- Mekaniskt skydd kring lokaler och utrymmen för att fördröja ett intrång
- Säkerhetstekniska system såsom larm-, kameraövervaknings- och passersystem

De olika åtgärderna ska dimensioneras och kravställas enligt branschnorm eller standard utifrån vilken information som hanteras på respektive plats. Förutom det fysiska skyddet krävs en fungerande tillträdeskontroll och utryckningstjänst.

Tabellen nedan ger övergripande riktlinjer för det fysiska skyddet vid förvaring av information i respektive informationssäkerhetsklass.

Informationssäkerhetsklass		**Riktlinjer för det fysiska skyddet**
K2 intern (sekretess)	Omslutningsytan: Tekniska säkerhetssystem:	Skyddsklass 2 enligt SSF 200 Larm i larmklass 2 enligt SSF 200
K3 sekretess	Omslutningsytan: Tekniska säkerhetssystem: Övrigt:	Skyddsklass 3 enligt SSF 200 Larm i larmklass 3 enligt SSF 200 Säkerhetsskåp SSF 3492
K4 hemlig	Omslutningsytan: Tekniska säkerhetssystem: Övrigt:	Skyddsklass 3 enligt SSF 200 Larm i larmklass 3 enligt SSF 200 Säkerhetsskåp SSF 3492

Tillträdeskontrollen syftar i första hand till att förhindra inbrott och stölder samt försvåra för obehöriga att få tillträde till utrymmen där sekretessbelagda och/eller hemliga uppgifter förvaras eller där säkerhetskänslig verksamhet bedrivs.

Kontrollen kan utföras med hjälp av säkerhetstekniska system såsom passersystem, larmsystem och kameraövervakning, sektionering av utrymmen (zonindelning) eller med hjälp

Processägare Direktör affärsstöd	Processledare/Uppdateringsansvarig Säkerhetschef	Kvalitetssamordnare Kvalitetschef	Skapat 2019-08-26	Senast ändrat 2021-06-15	Godkänt 2021-06-15

av säkerhetsskåp för förvaring. Kontrollen kan också utföras med hjälp av bevakningspersonal i vissa fall.

Då samtlig personal i ett byggprojekt använder ID-06 kan kortet användas som identitetsbärare i till exempel passer- och larmsystem.

Tabell nedan visar administrativa åtgärder som kan behöva hanteras i ett projekt.

Tillträdeskontroll	**Administrativa åtgärder att hantera**
Inpassering till kontor och byggarbetsplats	• Utfärdande av behörigheter till passersystemet. • Kortadministration. • Avslut av behörigheter.
Larm- och kameraövervaknings-system	• Aktivering och avaktivering av system. • Utfärdande av behörigheter till larm och kamerasystem. • Avtal som reglerar utryckningstjänst med inställelsetider för väktare. • Dokumentation och personuppgiftshantering (GDPR).
Sektionering	• Behörighet till olika områden. • Besökshantering.
Säkerhetsskåp	• Utfärdande av behörighet till säkerhetsskåp. • Eventuella samförvaringsbeslut. • Eventuell teknisk övervakning såsom larm.

Processägare Direktör affärsstöd	Processledare/Uppdateringsansvarig Säkerhetschef	Kvalitetssamordnare Kvalitetschef	Skapat 2019-08-26	Senast ändrat 2021-06-15	Godkänt 2021-06-15

Övergripande krav på IT-säkerhet

Information i informationssäkerhetsklass K1 och K2 får hanteras i molntjänster som godkänts av Locum.

Uppgifter i informationssäkerhetsklass K3 får endast hanteras i Locums servermiljö.

Säkerhetsskyddsklassificerade uppgifter, K4, kräver slutna system som är helt frånskilt internet eller vars åtkomst möjliggörs via signalskyddsåtgärder som godkänts av Försvarsmakten.

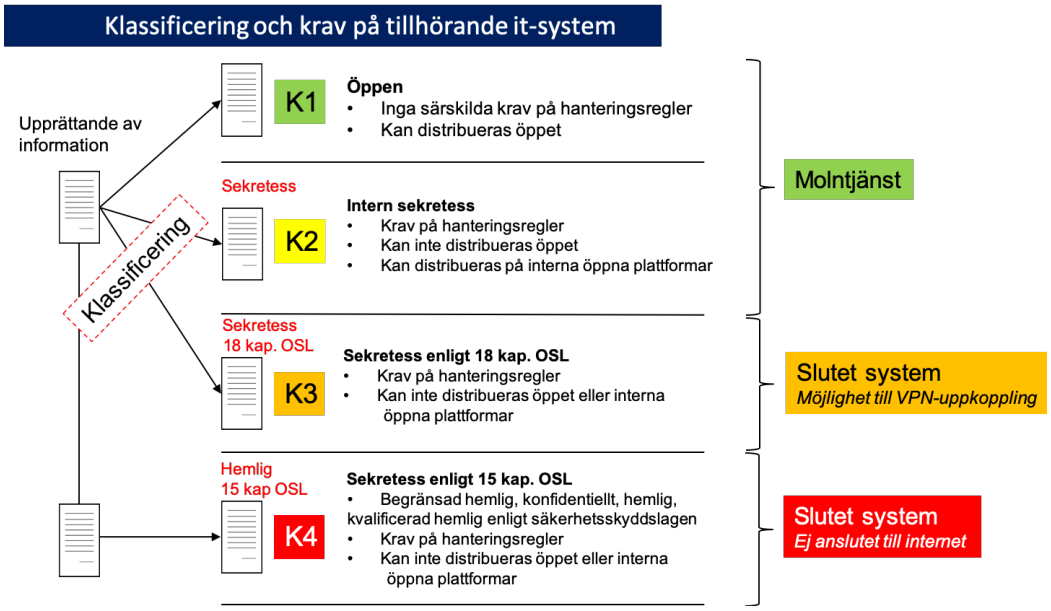


Illustration ovan: Översiktsbild visande informationssäkerhetsklasserna och övergripande krav på IT-säkerhet.

Säkerhetsrapportering

Incidenter som påverkar eller kan påverka informationssäkerheten för och kring projektet eller färdig byggnad ska rapporteras för att nödvändiga åtgärder ska kunna vidtas. Åtgärderna i sin tur syftar till att åtgärda brister, minimera skada samt eventuellt utreda inträffad skada.

Informationssäkerhetsincidenter ska skyndsamt anmälas till närmsta chef eller till projektets informationssäkerhetsspecialist för vidarebefordran till projektområdeschefen. Projektområdeschefen avgör om incidenten ska rapporteras till Locums säkerhetschef.

Exempel på händelser som ska rapporteras:

- Uppenbart felaktig hantering eller förlust av hemliga och/eller sekretessbelagda handlingar
- Misstanke om att obehörig kan ha fått del av hemlig och/eller sekretessbelagd handling
- Obehöriga som uppehåller sig i tillträdesbegränsat område
- Försök till inbrott eller inbrott i projektkontoret eller på byggarbetsplats

Processägare Direktör affärsstöd	Processledare/Uppdateringsansvarig Säkerhetschef	Kvalitetssamordnare Kvalitetschef	Skapat 2019-08-26	Senast ändrat 2021-06-15	Godkänt 2021-06-15

- Försök till inbrott eller inbrott i företagslokaler om dessa förvara sekretessbelagda och/eller hemliga handlingar
- Stöld av IT-utrustning eller dataintrång.

Kontrollverksamhet

Informationssäkerhetsspecialisten ansvarar för kontroller av informationssäkerheten och äger rätten att kontrollera externa granskare, projektörer och entreprenörer i projektet. Kontrollerna ska ske enligt upprättad kontrollplan.

Kontrollen ska säkerhetsställa att endast godkänd personal anlitas i projektet och att instruktionerna rörande informationssäkerhet och tillträdesbegräsning iakttas samt att skyddsnivån hos aktörerna är på föreskriven nivå. Kontrollerna ska dokumenteras.

Om kontrollen visar på brister i säkerhetsskyddet måste det omedelbart åtgärdas och rapporteras till Locums säkerhetschef.

Referenser

- Säkerhetsskyddslagen (2018:585).
- Säkerhetsskyddsförordningen (2018:658).
- Polismyndighetens författningssamling (PMFS 2019:2).
- Offentlighets- och sekretesslagen (2009:400).
- Riktlinjer för informationssäkerhet inom Stockholms läns landsting, 2015.
- Riktlinjer för informationssäkerhet, Locum, 2018.
- Informationssäkerhet Vägledning för medarbetare, Locum, 2018.
- Projekteringsanvisningar för teletekniska säkerhetssystem, Locum, 2016.
- Informationsklassificeringsguide för fastighetsinformation, Locum, 2019.
- Handbok Byggprojektledning, Locum, 2004.
- Handbok Skydd av byggnader, Fortifikationsverket, 2016.
- Handbok Säkerhetstjänst Fysisk säkerhet, Försvarsmakten, 2015.
- Handbok Säkerhetstjänst Grunder, Försvarsmakten, 2013.
- Säkerhetspolisen, www.sakerhetspolisen.se/sakerhetsskydd.