

Riktlinje för hantering av information i byggprojekt

Diarienummer: 2024-FA000122

Innehållsförteckning

Inledning.....	3
Syfte.....	3
Omfattning.....	3
Ansvar	4
Informationssäkerhet.....	4
Informationssäkerhetsklassificering	5
Att genomföra informationssäkerhetsklassificering	6
Praktisk hantering	6
Information i digital form	6
Information i analog form.....	7
Sekretess	8
Sekretessmarkering.....	9
Överföring och delning	10
Krav på avtal för säker hantering av information	11
Avtalsparters förhållande till sina underleverantörer	12
Utbildning och uppföljning	13
Versionshistorik riktlinje.....	15

Inledning

Denna riktlinje för hantering av information i byggprojekt är utformad för att säkerställa att all information som skapas och används inom Regionfastigheter, oavsett storlek på byggprojekt, hanteras på ett säkert och korrekt sätt. Riktlinjen omfattar ritningar, modeller och handlingar i både digital och analog form.

Syfte

Syftet med denna riktlinje är att skapa tydliga rutiner för säker informationshantering i Regionfastigheters byggprojekt. Riktlinjen ska bidra till att alla medarbetare följer gällande lagar, krav och interna regler för hantering av ritningar, modeller och handlingar, samt att sekretess och informationssäkerhet beaktas i hela projektets livscykel. Genom tydliga riktlinjer och processer ska denna dokumentation skapa förutsättningar för att information behandlas som en värdefull tillgång och att risker för obehörig åtkomst minimeras. Riktlinjen är en sammanställning av befintliga lagar och interna regler inom Region Skåne, med hänvisning till aktuella styrdokument.

Omfattning

Alla medarbetare inom Regionfastigheter, samt externa aktörer som entreprenörer och underleverantörer, omfattas av riktlinjen och har ett individuellt ansvar för korrekt hantering av information. Riktlinjen gäller vid delning, överföring och förvaring av ritningar, modeller och handlingar, oavsett om informationen är i digital eller analog form.

Riktlinjen omfattar även hantering av information som begärs ut enligt offentlighetsprincipen, där sekretessbedömning alltid ska göras innan information lämnas ut.

Ansvar

Projektchef eller projektledare ansvarar för att alla i projektet har tillgång till riktlinjen och vet hur den ska tillämpas. Vidare ansvarar projektchef eller projektledare för att i ett tidigt skede av byggprojektet klarlägga vilken information som omfattas av sekretess eller hög konfidentialitet, samt hur denna ska hanteras under projektets gång.

Varje medarbetare, såväl intern som extern part, har ansvar för att säkerställa att alla ritningar, modeller och handlingar som används i byggprojektet bedöms och hanteras korrekt i enlighet med denna riktlinje med avseende på sekretess och informationssäkerhet. Detta inkluderar att klassificera information, identifiera sekretessbelagda uppgifter och vidta rätt säkerhetsåtgärder vid hantering, lagring och delning.

Informationssäkerhet

Hantering av information i byggprojekt ska alltid utgå från principen om försiktighet. Med detta menas i korthet att om det råder någon osäkerhet kring hur information ska hanteras, ska man behandla den som om informationen omfattas av sekretess tills motsatsen är fastställd. Eftersom ritningar, modeller och handlingar i byggprojekt ofta innehåller känslig information, är det avgörande att alltid vara vaksam och säkerställa att informationen skyddas på rätt sätt. Genom att alltid skydda

information enligt riktlinjen minskar risken för obehörig åtkomst och informationsläckor.

Informationssäkerhetsklassificering

Informationssäkerhetsklassificering är en analys av vad konsekvenserna blir om informationen inte längre är konfidentiell, riktig eller tillgänglig. Varje parameter anges som ett värde mellan 1 och 4. Dessa förkortas som K (1–4), R (1–4) och T (1–4).

Konfidentialitet är det värde som avgör vem som är behörig att ta del av informationen. När en ritning, modell eller handling fått ett angivet värde för konfidentialitet som är K1, anses information vara öppen, det vill säga att konsekvensen om information skulle nås av obehöriga anses som ingen eller försumbar. Om värdet anges som K2 eller högre, måste sekretessprövning göras innan dokumentet delas med extern part.

Riktighet innebär att informationen ska skyddas mot oönskad förändring, oavsett om det är av obehöriga eller av misstag. Klassningen ska baseras på vad konsekvenserna blir om informationen inte längre är riktig.

Tillgänglighet är värdet som anger konsekvenserna om informationen inte är tillgänglig för behöriga användare. Det kan handla om avbrott i systemet, borttappade handlingar eller handlingar som raderats av misstag.

Värdena informationen klassas med ska ligga till grund för hur informationen hanteras i projektet. Om projektet bedömer att det leder till konsekvenser om informationen inte längre är

konfidentiell, riktig eller tillgänglig, krävs det att projektet vidtar säkerhetsåtgärder.

Att genomföra informationssäkerhetsklassificering

Vid klassificering av information finns stöd att tillgå på Region Skånes intranät: [Informationssäkerhetsklassificering - Region Skånes intranät](#)

Instruktion för vilka skalor och metoder som ska användas:
[Instruktion för informationsklassificering](#)

Informationsklassificeringen dokumenteras i:
[Mall: Beslut om informationssäkerhetsklassificering och fastställande av krav](#). Det är viktigt att informationen sedan hanteras med relevant skydd utifrån klassningen och att detta kommuniceras till berörda.

För ytterligare stöd gällande genomförande av informationsklassificering, kontakta Regionfastigheters informationssäkerhetssamordnare på enhet Fastighetsdigitalisering.

Praktisk hantering

Alla som hanterar ritningar, modeller och handlingar ska se dem som en värdefull tillgång och aldrig lämna dem obevakade.

Information i digital form

- Kontrollera alltid att de som får tillgång till ritningar, modeller eller handlingar är behöriga till informationen.

- Dela ritningar, modeller eller handlingar genom att länka till ett digitalt systemstöd som är informationsklassificerat.
- Använd säker e-post och dela endast små utsnitt av ritningar eller modeller vid absolut nödvändighet.
- Skydda elektroniska sekretessmarkerade ritningar, modeller och handlingar med lösenord, kryptering eller annan säkerhetsteknik för att förhindra obehörig åtkomst.
- Dator eller annan enhet ska alltid låsas när du inte arbetar vid den.

Information i analog form

- Kontrollera alltid att de som får tillgång till ritningar, modeller eller handlingar är behöriga till informationen.
- Förvara alltid analoga ritningar, modeller och handlingar inlåsta när de inte används.
- Fysiska kopior av sekretessmarkerade ritningar, modeller eller handlingar ska förstöras på ett säkert sätt när de inte längre behövs i projektet.
- Sekretessmarkerade ritningar, modeller eller handlingar ska förvaras på ett säkert sätt för att förhindra obehörig åtkomst. Detta kan inkludera låsta skåp.
- Innan du lämnar arbetsplatsen eller mötesrum, kontrollera att inga ritningar, modeller eller handlingar ligger kvar.

Sekretess

Sekretessbelagd information får inte delas, varken muntligen eller genom att lämna ut handlingar. När det i ritningar, modeller och handlingar finns information som omfattas av sekretess ska handlingarna endast vara tillgängliga för personer som behöver dem i sitt arbete eller enligt avtal med Regionfastigheter.

Offentlighets- och sekretesslagen (OSL) innehåller bestämmelser som skyddar allmänna intressen genom sekretess. Lagen innehåller även bestämmelser om myndigheters skyldighet att registrera allmänna handlingar samt regleringar för när en handling får lämnas ut¹. I nedan länkad riktlinje finns instruktioner på hur man går till väga för att bedöma om en ritning, modell eller handling bör omfattas av sekretess, samt hur man praktiskt utför maskeringen av information:

[Sekretesspröva allmänna handlingar för handläggare](#)

Om begäran för utlämnande av handling avser upphandling under avtalsspärr ska denna riktlinje följas:

[Instruktion - hantera begäran lämna ut handlingar](#)

Exempel på information som ofta omfattas av sekretess:

- Uppgifter om upphandlingar och/eller leverantörer
- Säkerhetsrelaterade dokument
- Riskanalyser av olika slag
- Vårduppgifter
- Markhandlingar och installationsplaner
- Uppgifter om teknisk infrastruktur

¹ [Offentlighets- och sekretesslag \(2009:400\) | Sveriges riksdag](#)

- Affärskritiska uppgifter

Ovan är några exempel på tillfällen då det ofta förekommer sekretess. Om ritningen, modellen eller handlingen innehåller något av ovanstående uppgifter är det stor sannolikhet att det förekommer sekretess. Det betyder däremot inte att det är så i alla situationer, eller att exemplen ovan är heltäckande.

Sekretessmarkering

När en ritning, modell eller handling innehåller information som omfattas av sekretess, ska denna markeras med en sekretessmarkering.

Sekretessmarkeringen visar att informationen omfattas av särskilda regler och inte får delas utan behörighetsprövning. Sekretesstämplar ska innehålla tydlig information om vilken typ av sekretess som gäller, inklusive hänvisning till den relevanta delen av offentlighets- och sekretesslagen.

Den officiella stämpeln görs av diariet på Region Skåne i samband med att en handling diarieförs. Stämpeln innehåller en hänvisning med kapitel och paragraf till offentlighets- och sekretesslagen för tillämpad sekretessbestämmelse, datum som anger när stämpeln sattes på handlingen samt vilken myndighet som stämplat den. Notera att hänvisningen till offentlighets- och sekretesslagen i stämpeln varken är fullständig eller uteslutande, fler lagrum än det som anges kan vara aktuellt. Stämpeln ser ut så här:

Sekretessmarkering
Sekretess enl. 18 kap. 13§ Offentlighets- och sekretesslag (2009:400) 2023-10-20 Region Skåne

För digitala ritningar, modeller eller handlingar som ännu inte diarieförts, ska den angivna stämpeln ovan användas fram tills dess att handlingen diarieförs. Stämpeln finns i projektens projekthandbok och bör placeras på den sekretessbelagda ritning, modell eller handlings första sida.

Analoga ritningar, modeller och handlingar som ännu inte diarieförts ska märkas som "Sekretessmarkering" följt av datum för när sekretessbedömningen gjordes. Markeringen kan göras genom att skriva manuellt, det viktigaste är att den framgår tydligt.

Varje gång en handling begärs ut ska sekretessprövning genomföras. Markeringen är en notering om att handlingen kan innehålla uppgifter om sekretess, men informationen är inte maskerad. Maskering sker först då den ska lämnas ut.

Överföring och delning

När sekretessbelagd information ska överföras eller delas, ska alltid säkra kommunikationskanaler användas. Exempel på detta är krypterad e-post eller informationssäkerhetsklassificerade filöverföringstjänster. Ritningar, modeller och handlingar ska endast delas via system som är klassificerade för att hantera känslig information. Vid delning utanför organisationen ska alltid sekretessprövning göras innan material lämnas ut.

Vid delning av både digital och analog information är det viktigt att kontrollera att de som får tillgång till ritningar, modeller eller handlingar är behöriga till informationen.

Endast system som är informationssäkerhetsklassificerade får användas för lagring, hantering och delning av känslig information i byggprojekt. Det innebär att alla system som används för lagring, hantering och överföring av information måste vara bedömda och klassificerade för att hantera olika nivåer av känslighet och sekretess.

Kontakta enhet Fastighetsdigitalisering på VO Fastighetsutveckling, vid frågor om systemklassificering för känslig information.

Krav på avtal för säker hantering av information

Regionfastigheter har i processen för upphandling säkerställt att de allmänna bestämmelserna (AB 04, ABT 06, ABK 09) reglerar Regionfastigheters rätt till informationen i byggprojekt. Alla upphandlingsavtal ska inkludera tydliga sekretesskrav för leverantörer.

Alla byggprojekt ska använda Regionfastigheters mallar och följa upphandlingsprocessen.

Här återfinns [Upphandlingsprocessen](#) på Region Skånes intranät.

Avtalsparters förhållande till sina underleverantörer

Regionfastigheters avtalsparters ansvarar för att deras underleverantörer följer sekretesskrav och hanterar information enligt riktlinjen.

Detta innebär bland annat att entreprenören, dennes anställda, och/eller anlitad personal inte i någon form får vidarebefordra eller röja information om Region Skåne, vare sig den skulle gälla patienter eller kunder, ekonomiska eller affärsmässiga förhållanden, system- och IT-lösningar, säkerhetsåtgärder, anställda eller leverantörer registrerade hos Region Skåne.

Sekretessen innebär också att entreprenören inte heller får befatta sig med uppgifter, vidarebefordra information eller ta kontakter med utomstående som inte har samband med entreprenaden. Detta gäller all sekretessinformation, såväl muntlig som skriftlig och både formell och informell, såvida den inte är uppenbart klassad som publik, det vill säga allmänt tillgänglig information.

Entreprenören förbinder sig:

- Att informera berörd personal samt underentreprenörer, som entreprenören ansvarar för, om sekretessens innebörd.
- Att varken under eller efter entreprenadens fullgörande obehörigen röja sådan information som angetts ovan.
- Att säkerställa att alla anställda och underleverantörer undertecknar en tystnadspliktsförbindelse.
- Vid entreprenadens slut ska all sekretessbelagd information återlämnas.

- Att i övrigt följa Region Skånes anvisningar för hantering av patient- respektive personuppgifter
Informationssäkerhet: [Personuppgiftsbehandling i Region Skåne - Sammanställning av regler och krav](#)

Entreprenören ska på begäran redovisa hur sekretessbelagd information hanteras.

Om tveksam tolkning av denna sekretessförbindelse skulle uppkomma ska förtydligande inhämtas omgående via beställaren.

Utbildning och uppföljning

Linjeförord ansvarar för att medarbetare regelbundet utbildas i säker informationshantering, inklusive hantering av sekretessmarkerade ritningar, modeller och handlingar.

Obligatoriska utbildningar i Lärportalen:

[Säker informationshantering - Lärportalen](#)

[IT- och cybersäkerhet i Region Skåne](#)

Regionfastigheters arkivansvarig genomför regelbundna kontroller av hur verksamhetsinformation hanteras, inklusive sekretessmarkerade ritningar, modeller och handlingar. Detta sker enligt Region Skånes instruktion för mätning av mognadsnivåer:

[Mätning av mognadsnivåer för hantering av verksamhetsinformation.](#)

Arkivansvarig ansvarar för att regelbundet granska och uppdatera riktlinjen så att den följer gällande regler och krav. Frågor om riktlinjen eller hantering av sekretessbelagd

information hänvisas till Regionfastigheters arkivansvarig på
Enhet kvalitet och hållbarhet.

Mer information om informationssäkerhet finns på Vårdgivare
Skåne: [Informationssäkerhet - Vårdgivare Skåne](#)

Versionshistorik riktlinje

Versionshistoriken sammanfattar viktiga ändringar i riktlinjen för att säkerställa transparens och spårbarhet.

Version	Datum	Beslut	Ändringar
1.0	2024-07-04	Fastighetsdirektör Pål Svensson	Riktlinje upprättad. Framarbetad i samarbete inom Regionfastigheter bestående av informationsspecialist för fastighetsinformation, informationssäkerhetsstrateg, säkerhetsansvarig samt arkivansvarig.
2.0	2024-09-25	Fastighetsdirektör Pål Svensson	Ansvarsfördelningen har förtydligats och titeln projektchef används nu samlingsbegrepp för den roll som har högsta ansvaret i ett byggprojekt (ibland projektledare). Tillägg att avsteg från riktlinjen ska dokumenteras och hanteras i enlighet med Regionfastigheters process för avstegshantering. Därutöver har vissa språkliga förändringar gjorts.
3.0	2025-02-14		Efter remissrunda har riktlinjens struktur och innehåll omarbetats för ökad tydlighet. Länkar till relevanta styrdokument, riktlinjer och instruktioner har lagts till.
3.0	2025-03-20		Efter remissrunda i LG och Upphandlingsenheten har riktlinjens innehåll och formuleringar justerats.
3.0	2025-03-31		Beslut i LG om implementering av riktlinjerna.