# Förord

Flertalet av de smarta produkter och tjänster som utvecklas och marknadsförs inom fastighetssektorn bygger på åtkomst till kontinuerligt insamlade dataströmmar. Det kan gälla data om byggnaders energi- och vattenflöden, luftkvalitet och konstruktiva tillstånd, men också data om de aktiviteter som genomförs i eller i nära anslutning till byggnaden.

Syftet med denna vägledning är att beskriva hur man, med utgångspunkt i ett systematiskt informationssäkerhetsarbete, kan utveckla en organisatorisk förmåga att möta efterfrågan på denna typ av dataströmmar.

Primär målgrupp för skriften är kommunernas säkerhetsorganisationer och fastighetsorganisationer. Sekundär målgrupp är övriga fastighetsägare, konsulter och leverantörer som verkar inom fastighetsbranschen.

Projektet har finansierats av FoU-fonden för kommunernas fastighetsfrågor. Thomas Nilsson och Eilia Etminan, Certezza AB samt Lars Lidén, Meta fastighetsadministration har varit utredare. Lisa Knutsson Fröjd, Region Gävleborg och Henrik Bjerneld, Härnösands kommun har generöst delat med sig av erfarenheter inom kunskapsdomänen processorienterad informations-kartläggning.

Mats Carlqvist, SISAB; Stefan Albrekt, Hörby kommun och Andreas Persson, AB Familjebostäder har ingått i styrgruppen och har bidragit med konkreta exempelfall och insikter inom området. Bo Baudin, Sveriges Kommuner och Regioner har varit projektledare.

Tack till alla som deltagit i arbetet med framtagandet av skriften!

Stockholm i januari 2022

| | |
|---|---|
| Gunilla Glasare | Peter Haglund |
| Avdelningschef | Sektionschef |

*Avdelningen för Tillväxt och samhällsbyggnad*

# Innehåll

# Inledning

## Bakgrund

Inom näst intill varje verksamhetsområde ställs allt högre krav på ett systematiskt informationssäkerhetsarbete. Allt från regulatoriska krav till olika former av interna och externa krav, inte minst vid samverkan. Typiskt är också att informationssäkerhetsarbetet ofta är eftersatt och att kunskapen om den aggregerade informationsmängdens värde och de konsekvenser det får om informationen är inkorrekt eller hamnar i orätta händer kan leda till ökade hot mot samhället.

## Syfte och målgrupp

Syftet med detta initiativ har varit att stödja fastighetsbranschens aktörer genom att bidra med normerande vägledningsmaterial för det systematiska informationssäkerhetsarbetet med fokus på informationsklassning för strömmande data.

Primär målgrupp är kommunernas säkerhetsorganisationer och fastighetsorganisationer. Sekundär målgrupp är övriga fastighetsägare, konsulter och leverantörer som verkar inom fastighetsbranschen.

## Effektmål

Normering av informationsklassningsmodeller för vanligt förekommande tjänster inom fastighetsförvaltning:

- förenklar informationsutbyte inom och mellan organisationer
- särskild belysning av aggregerade informationsmängder
- likartad kravställning vilket också leder till en ökad medvetenhet hos leverantörerna
- minskad risk att skyddsvärd information hamnar i orätta händer eller är inkorrekt

## Projektmål och leverabler

Målet har varit att ta fram denna vägledning för att stödja kommunernas systematiska informationssäkerhetsarbete inom sektorn fastighetsförvaltning och samtidigt bidra till en totalt sett ökad mognadsgrad i kommunerna.

Ett annat mål ha varit att förse KLASSA[1] med stödmaterial för informations-klassning inom kommunal fastighetsförvaltning med denna vägledning som grund. Stödmaterialet kan självklart också användas av organisationer som inte använder KLASSA. Stödmaterial som publiceras på KLASSA:s webbplats förvaltas av KLASSA-förvaltningsorganisation.

[1] Klassa, Informationsklassning (https://skr.se/skr/naringslivarbetedigitalisering/digitalisering/arkitektursakerhet/informationssakerhet/klassainformationsklassning.7558.html)

# Termer och begrepp

I denna rapport används en rad termer och begrepp relaterade till informationssäkerhet. Vi har valt att beskriva följande termer och begrepp för att skapa en tydlighet för läsaren.

## Säkerhetsaspekter

| Säkerhetsaspekt | Definition i SIS Handbok 550 | Definition i SS-ISO/IEC 27001 |
|---|---|---|
| Konfidentialitet | Skyddsmål att innehållet i informationsobjekt (eller ibland dess existens) inte får göras tillgängligt eller avslöjas för obehöriga | Egenskapen att information inte tillgängliggörs eller avslöjas till obehöriga individer, enheter eller processer |
| Riktighet | Skyddsmål att information inte förändras, vare sig obehörigen, av misstag eller på grund av funktionsstörning | Egenskapen att skydda exaktheten och fullständigheten gällande tillgångar |
| Tillgänglighet | Skyddsmål där informationstillgångar ska kunna utnyttjas i förväntad utsträckning och inom önskad tid | Egenskapen att vara åtkomlig och användbar vid begäran av behörig enhet |

## Begrepp

| Begrepp | Beskrivning |
|---|---|
| Information & data | Data består i första hand av text och siffror medan information är förädlad data som människor förstår. Utan att särskilja information och data så är information text, bild, mätdata, siffror, rapporter, statistik, tal, ljud och mycket mer. |
| Strömmande data | En dataström är en informationssekvens som skickas mellan två enheter. En dataström består av många små paket eller pulser. Var och en av dessa paket eller pulser innehåller en liten mängd information. När de kombineras utgör de hela den skickade informationen. Denna process kallas dataöverföring. |
| Informationssystem | Applikationer, tjänster eller andra komponenter som hanterar information. I begreppet ingår också nätverk och infrastruktur. |
| Informationstillgång | Innefattar både den information, och de informationssystem som hanterar informationen, som är av värde för en organisation. |
| Informationsägare | Den person, eller funktion, som har ansvaret för den information som skapas och hanteras inom den egna organisationen. |

# Allmänt om informationsklassning

Syftet med informationsklassning är att skapa en grundläggande förståelse för hur skyddsvärd en viss informationsmängd är, det vill säga hur viktigt det är att informationen är korrekt, att den inte förvanskas avsiktligt eller oavsiktligt samt att den är tillgänglig när den behövs.

Förenklat innebär det att tre perspektiv belyses enligt följande:

- Konfidentialitet – Vad blir skadan om informationen hamnar i orätta händer?
- Riktighet – Vad blir skadan om informationen inte är korrekt?
- Tillgänglighet – Vad blir skadan om informationen inte är tillgänglig?

I arbetet med denna vägledning har fokus i första hand varit på strömmande data, men modeller, metodik och tillvägagångssätt ska i möjligaste mån inte skilja sig åt för olika typer av information eller hur de hanteras då det skulle bli ogörligt att ha ramar för det systematiska informationssäkerhetsarbetet. Därför har fokus lagts på att beskriva ”ledstången att hålla sig i”, men att med exempel beskriva hur utmaningar avseende strömmande data bäst hanteras.

## Verktyget KLASSA och metodiken för informationsklassning

I denna rapport refererar vi en hel del till SKR:s verktyg KLASSA då det till stor del är normerande för SKR:s medlemmars informationssäkerhetsarbete. Det innebär inte att resonemang och exempel inte är tillämpningsbara för dem som inte använder KLASSA.

KLASSA är ett verktyg som togs fram av SKR under 2012 efter ett arbete i Stockholmsregionen med att skapa samsyn kring bland annat informations-klassning och hur resultatet av informationsklassningen också fastställer ett minimikrav för hur informationen ska skyddas.

SKR:s syfte med att tillhandahålla och vidareutveckla KLASSA är att bidra till att öka mognadsgraden inom informationssäkerhet hos SKR:s medlemmar och inte enbart avgränsat till informationsklassning. Det innebär att KLASSA successivt breddas till att stötta arbetet inom exempelvis riskhantering, kontinuitetsplanering och incidenthantering.

KLASSA utgår från standarderna SS-ISO/IEC 27001 och 27002 som beskriver en modell och metodik för informationsklassning. Dessa standarder och MSB:s metodstöd har legat till grund för SKR:s verktyg KLASSA. SKR har utformat modellen så att dess medlemmar kan klassa informationstillgångar på ett likartat sätt och i syfte att skapa en gemensam förståelse för krav på skydd och för tillämpningen av lämpliga skydd.

De konsekvensnivåer som används i KLASSA följer den modell[2] för klassificering av information som utarbetats av MSB och Svenska Institutet för Standarder (SIS):

- Synnerligen allvarlig skada (4)
- Allvarlig skada (3)
- Betydande skada (2)
- Måttlig skada (1)
- Försumbar skada (0)

**Synnerligen allvarlig skada (4)** definierades inte i arbetet av SIS/MSB. I takt med den ökade hotbilden i omvärlden såg SKR och flera av dess medlemmar ett ökande behov av att uppmärksamma dessa informationstillgångar varför den infördes redan år 2013 i KLASSA version 1 som en indikation på att informationstillgången berörs av säkerhetsskyddslagen (2018:585).

I denna vägledning har vi utgått från de konsekvensnivåer som finns i KLASSA. Vi har också haft en dialog med Lantmäteriet mot bakgrund av arbetet med en obruten digital samhällsbyggnadsprocess där översiktsplaner, detaljplaner och bygglov ingår. Syftet har varit att stämma av konsekvensnivåerna för informationsklassning för att se om de utgör några hinder i den gemensamma synen på hur information ska klassas. Uppfattningen är att de harmoniserar väl med hur konsekvensnivåerna i KLASSA uttrycks. För närmare förklaring av konsekvensnivåernas betydelse se KLASSA:s stödmaterial[3]. Där finns också översättningar till fler modeller som beskriver konsekvensnivåer.

[2] Modell för klassificering av information (https://www.msb.se/RibData/Filer/pdf/25602.pdf)
[3] SKR KLASSA stödmaterial (https://klassa-info.skr.se/stodmaterial)

I kommande avsnitt finns grundläggande vägledning för val av konsekvensnivå kopplat till de vanligt förekommande regulatoriska kraven.

## KLASSA och strömmande data

Det har inte varit självklart att se KLASSA som ett verktyg och ett stöd för att hantera tillämpningar med strömmande data. KLASSA inriktades inledningsvis mot system, inte information eller strömmande data. Mot bakgrund av detta tog SKR ett initiativ under 2019/2020 och visade hur KLASSA kan användas i olika IoT-tillämpningar för att med samma modell och metodik informations-klassificera och påföra skyddsåtgärder som ett resultat av informationens skyddsvärde.

Exempel på IoT-tillämpningar som belystes i projektet KLASSA för IoT var:

- Smart och uppkopplad belysning[4]
- Smart trafikstyrning[5]
- Upphandling av IoT-plattform[6]

För närmare information se SKR:s rapport KLASSA för IoT[7]

Under arbetet med KLASSA för IoT visade det sig att det fanns delar i KLASSA som inte gick att applicera fullt ut. I huvudsak bestod utmaningarna i att KLASSA:s förslag på skyddsåtgärder, som inspirerats av de normativa kraven i SS-ISO/IEC 27001, var formulerade på ett sådant sätt att de inte alltid var applicerbara på den här typen av informationstillgångar. I ett parallellt projekt inom SKR pågick då utvecklingen av KLASSA version 4 som bland annat ersatte KLASSA:s hittills systemcentriska fokus med ett informations-centriskt fokus. I samband med denna transformering hörsammades också de brister som uppmärksammades i initiativet KLASSA för IoT och därför gicks kontroll- och kravkatalogen igenom för att göra förslagen på skyddsåtgärder oberoende av i vilket sammanhang de existerar. Denna brist är således hanterad i KLASSA version 4.

[4] Stockholms stad - Smart och uppkopplad belysning (https://smartstad.stockholm/smart-och-uppkopplad-belysning/)
[5] Smart stad trafikstyrning (https://smartstad.stockholm/smart-trafikstyrning/)
[6] Smart stad IoT (https://smartstad.stockholm/iot-stockholm/)
[7] KLASSA för IoT (https://webbutik.skr.se/sv/artiklar/klassa-for-iot.html)

förenad med. Säkerhetspolisens vägledning[11] i säkerhetsskydd med fokus på informationssäkerhet ger också rekommendationer inom området.

En säkerhetsskyddsanalys används för att identifiera om och i vilken utsträckning verksamheten är av betydelse för Sveriges säkerhet eller hanterar information som omfattas av säkerhetsskyddslagen. Säkerhetsskyddsanalysen ska utreda behovet av säkerhetsskydd. Med utgångspunkt i analysen ska verksamhetsutövaren planera och vidta de säkerhetsskyddsåtgärder som behövs med hänsyn till verksamhetens art och omfattning, förekomst av säkerhetsskyddsklassificerade uppgifter och övriga omständigheter. Säkerhetsskyddsåtgärderna delas in i tre delar: informationssäkerhet, fysisk säkerhet och personalsäkerhet. Se vidare säkerhetspolisens information om säkerhetsskydd[12]

Det pågår arbete med att utveckla KLASSA till att också vara ett stöd för klassning enligt säkerhetsskyddslagen. Det kan komma att implementeras i framtida versioner.

### Lagen om informationssäkerhet för samhällsviktiga och digitala tjänster (NIS-lagen och kommande uppdatering av NIS-direktivet)

NIS-lagen gäller för verksamheter inom någon av sektorerna

- energi,
- transport,
- bankverksamhet,
- finansmarknadsinfrastruktur,
- hälso- och sjukvård,
- leverans och distribution av dricksvatten, eller
- digital infrastruktur.

Lagen gäller för leverantörer som är etablerade i Sverige och där tillhandahållandet av tjänsten är beroende av nätverk och informationssystem (NIS) och en incident skulle medföra en betydande störning vid tillhandahållandet av tjänsten.

---

[11] Säkerhetspolisens vägledning (https://www.sakerhetspolisen.se/download/18.f2735ce171767402ba3dc/1599633194948/Vagledning-Informationssakerhet_2020.pdf)

[12] Säkerhetspolisen om säkerhetsskydd (https://www.sakerhetspolisen.se/sakerhetsskydd.html)

MSB har preciserat kriterierna för när en verksamhet omfattas av regelverket i Myndigheten för samhällsskydd och beredskaps föreskrifter om anmälan och identifiering av leverantörer av samhällsviktiga tjänster (MSBFS 2018:7)[13].

NIS-lagen implementerar EU:s direktiv om åtgärder för en hög gemensam nivå på säkerhet i nätverks- och informationssystem i hela unionen (NIS-direktivet). I slutet av 2020 presenterade EU-kommissionen ett förslag på ett nytt NIS-direktiv, kallat NIS 2. Syftet med det reviderade förslaget är att anpassa direktivet till nya och framtida behov. Förslaget har inte fastställts, utan har lämnats för beredning till rådet och EU-parlamentet. Om förslaget fastställs i dess nuvarande lydelse kommer NIS-lagen att behöva anpassas till förändringarna. NIS-regleringens tillämpningsområde kommer därmed att utökas till att även omfatta bland annat

- molntjänstleverantörer,
- statliga myndigheter, vissa regioner och enstaka kommuner,
- distributörer av fjärrvärme,
- företag inom avlopps- och avfallshantering och
- produktions- och tillverkningsindustri inom livsmedel, läkemedel, biogas, fordon, kemikalier, datorer, maskiner och verktyg.

Fastighetsägare utgör inte sådan aktör som direkt omfattas av NIS-regelverket. Att äga och förvalta en anläggning eller byggnad medför inga krav ur ett informationssäkerhetsperspektiv.

Fastighetsägaren kan emellertid bli indirekt påverkad av NIS-regelverket. Det är möjligt att hyresgäster som berörs av regulatoriska krav på sin informationssäkerhet (genom bl.a. NIS eller säkerhetsskyddslagen (2018:585)) kan komma att ställa krav på att anläggningen eller byggnaden de hyr dimensioneras i enlighet med regleringen. Sådana krav på säkerhetsåtgärder bör ställas av hyresgästerna i upphandlingsskedet, men kan även tillkomma vid avtalsförnyelse. Säkerhetsåtgärderna bör syfta till att reducera verkningar av sådana konsekvenser som hyresgästerna identifierat i de riskanalyser som NIS-lagen kräver (12 §).

[13] MSB:s föreskrifter om anmälan och identifiering av leverantörer av samhällsviktiga tjänster (https://www.msb.se/siteassets/dokument/regler/rs/0264c176-6b31-43c6-9fd8-807102df3844.pdf)

På samma sätt kan fastighetsägare komma att påverkas indirekt genom att deras samverkanspartners i närliggande branscher (exempelvis avlopps- och avfallshantering, eldistribution, fjärrvärme) berörs av det föreslagna regelverket NIS 2 och att de i sin tur ställer nya krav på säkerhet i samarbetet. Det kan leda till ökade samarbets- och leveranskostnader för fastighetsägarna.

Ett potentiellt hål i NIS 2 avser it-system för fastighetsautomation. Fastighetsägare kan installera it-system för fastighetsautomation för att reglera värme- och kyla på distans. Systemen för fastighetsautomation kan utsättas för attacker med allvarliga konsekvenser för hyresgästerna med potentiell inverkan på samhället i stort. Direktivförslaget NIS 2 omfattar aktörer som distribuerar fjärrvärme eller fjärrkyla via ett nät till flera byggnader eller anläggningar, men inte kunderna (i detta fall fastighetsägarna) som ansvarar för reglaget av fjärrvärmen och -kylan.

Störningar som får en betydande inverkan på kontinuiteten i dessa tjänster ska rapporteras till MSB. I MSB:s föreskrift om rapportering av incidenter för leverantörer av samhällsviktiga tjänster (MSBFS 2018:9)[14] har myndigheten i detalj definierat vad som innebär betydande störning för dessa verksamheter.

I de allra flesta fall kommer informationstillgångar som omfattas av NIS-lagen att klassas på nivån **betydande (2)** eller **allvarlig (3)** för samtliga säkerhetsaspekter, dels för att tjänsterna är samhällsviktiga, dels eftersom konsekvensnivåerna är så tydligt definierade i föreskrifterna.

### EU:s Dataskyddsförordning (GDPR)

Dataskyddsförordningen syftar till att skydda levande, fysiska personers grundläggande rättigheter och friheter, särskilt deras rätt till skydd av personuppgifter. Enligt dataskyddsförordningen ska den som är personuppgiftsansvarig vidta lämpliga tekniska och organisatoriska åtgärder för att säkerställa en säkerhetsnivå som är lämplig i förhållande till risken.

Personuppgifter är alla uppgifter som avser en identifierad eller identifierbar fysisk person. Med identifierbar menas att även indirekta uppgifter omfattas av dataskyddsförordningens tillämpningsområde. Personuppgifter kan behöva olika skyddsåtgärder beroende på vilken typ av uppgift det rör sig om eller i vilket sammanhang den förekommer. Vanligt förekommande personuppgifter

[14] MSB:s föreskrift om rapportering av incidenter för leverantörer av samhällsviktiga tjänster (https://www.msb.se/siteassets/dokument/regler/forfattningar/msbfs2018_9.pdf)

kan till exempel behöva ett högt skydd om det handlar om skyddade personuppgifter eller mycket omfattande personuppgifter. Utöver detta har Integritetsskyddsmyndigheten identifierat vissa kategorier av personuppgifter som kräver extra skydd.

**Extra skyddsvärda personuppgifter – personnummer**

Personnummer är enligt Integritetsskyddsmyndigheten (IMY) en extra skyddsvärd uppgift som bör behandlas i så liten utsträckning som möjligt.

**Särskilt skyddsvärda personuppgifter – integritetskänsliga personuppgifter**

Integritetsskyddsmyndigheten har identifierat vissa typer av uppgifter som myndigheten anser är särskilt skyddsvärda. Exempel på sådana uppgifter är löneuppgifter, uppgifter om lagöverträdelser, värderande uppgifter från utvecklingssamtal, resultat från personlighetstester, information som rör någons privata sfär och uppgifter om sociala förhållanden, uppgifter om ekonomisk hjälp eller insatser inom socialtjänsten. Dessa uppgifter hanteras normalt enligt en högre säkerhetsnivå än mindre känsliga uppgifter.

**Känsliga personuppgifter**

Dataskyddsförordningen identifierar särskilt vissa kategorier av personuppgifter som känsliga och som av den anledningen kräver en högre säkerhetsnivå. Dessa uppgifter är:

- ras eller etniskt ursprung
- politiska åsikter
- religiös eller filosofisk övertygelse
- medlemskap i fackförening
- hälsa eller sexualliv
- genetiska uppgifter, biometriska uppgifter för att entydigt identifiera en fysisk person

Några punkter att beakta i arbetet med att klassificera informationen är bland annat om något av följande behandlas:

- uppgifter om personer med skyddade personuppgifter
- uppgifter om enskildas sociala eller ekonomiska förhållanden
- personuppgifter om ett stort antal personer

- personnummer eller samordningsnummer
- en stor mängd personuppgifter om varje person

Enligt dataskyddsförordningen är en personuppgiftsincident ”en säkerhetsincident som leder till oavsiktlig eller olaglig förstöring, förlust eller ändring eller till obehörigt röjande av eller obehörig åtkomst till de personuppgifter som överförts, lagrats eller på annat sätt behandlats”. Det innebär att personuppgifter måste hanteras på ett korrekt sätt gällande alla säkerhetsaspekter. Inte bara konfidentialitet, utan även aspekten tillgänglighet måste vägas in liksom riktighet.

Med sannolikhet hamnar vanliga personuppgifter i klassificeringen **betydande (2)** för samtliga säkerhetsaspekter. I sammanhang där särskilda kategorier (känsliga personuppgifter och integritetskänsliga personuppgifter) behandlas är klassificeringen **allvarlig (3)** för säkerhetsaspekten konfidentialitet och i vissa fall även riktighet.

### Personuppgifter inom hälso- och sjukvården

Patientdatalagen (2008:355) (PDL) tillämpas på vårdgivares behandling av personuppgifter inom hälso- och sjukvården. I Socialstyrelsens föreskrifter och allmänna råd om journalföring och behandling av personuppgifter i hälso- och sjukvården (HSLF-FS 2016:40) finns krav om att överföring av personuppgifter i öppna nät ska göras på ett sådant sätt att ingen obehörig kan ta del av uppgifterna och att åtkomst till uppgifterna ska föregås av stark autentisering. Vårdgivaren ska säkerställa att uppgifter i en patientjournal inte kan ändras eller utplånas annat än med stöd av PDL.

Patientdata utgör generellt sett känsliga personuppgifter och normalt klassificeras dessa i konsekvensnivån **allvarlig** för säkerhetsaspekten konfidentialitet. I sammanhang med mycket höga krav på riktighet, exempelvis ordinationer, är klassificeringen **allvarlig** för säkerhetsaspekten riktighet.

### Sekretessreglerade uppgifter

En handling är en framställning i skrift eller bild samt en upptagning som endast med tekniska hjälpmedel kan läsas eller avlyssnas eller uppfattas på annat sätt. En handling innehåller därmed vissa uppgifter.

En handling är allmän, om den förvaras hos en myndighet och är inkommen till eller upprättad hos en myndighet.

En allmän handling är antingen offentlig eller omfattas helt eller delvis av sekretess.

Sekretess innebär ett förbud att röja en uppgift, vare sig det sker muntligen, genom utlämnande av allmän handling eller på något annat sätt. Sekretess-belagda uppgifter kan vara uppgifter i allmänna handlingar men också uppgifter som inte ingår i en allmän handling, till exempel uppgifter som finns i en handling som ännu inte upprättats hos en myndighet.

**Det finns tre typer av sekretess; absolut, stark och svag:**

- Absolut sekretess betyder att inga uppgifter under några förutsättningar får lämnas ut till andra än de anställda som behöver uppgifterna för att kunna utföra sitt arbete. Detta gäller t.ex. för uppgifter i ännu inte avslutade upphandlingsärenden och uppgifter inom kommunal familjerådgivning som enskild lämnar i förtroende eller som inhämtats i förtroende.
- Stark sekretess betyder att sekretess är huvudregeln och uppgiften får endast lämnas ut om det står klart att så kan ske utan att visst men eller viss skada uppkommer.
- Svag sekretess betyder att offentlighet är huvudregeln och uppgiften omfattas av sekretess om det kan antas att visst men eller viss skada kan uppstå.

Sekretessreglerade uppgifter påverkar endast skyddsnivån konfidentialitet. Skyddsmålen för riktighet och tillgänglighet regleras inte i offentlighets- och sekretesslagen (2009:400).

Konfidentialitet medför inte automatiskt sekretess, även om det kan finnas en koppling. Sålunda ska de två begreppen (konfidentialitet och sekretess) hållas åtskilda. Det kan innebära att allmänna handlingar som är offentliga och som skulle lämnas ut till en enskild vid begäran om utlämnande av allmän handling trots detta inte bör ges den lägsta konsekvensnivån (”ingen eller försumbar”) när det gäller konfidentialitet.

Omständigheter att beakta vid klassning av sekretessreglerade uppgifter är vilken skada som kan uppstå om uppgifterna röjs för obehörig samt om det gått

lång tid sedan uppgifterna sekretessbelades och det är kort tid kvar av den skyddstid för vilken sekretessen gäller. Det innebär att konsekvensnivån kan variera från **måttlig (1), betydande (2), allvarlig (3)** eller **synnerligen allvarlig (4)** för säkerhetsaspekten konfidentialitet.

### Arkivlagen (1990:782)

Av arkivlagen (1990:782) framgår bland annat att i arkivvården ingår att myndigheten ska organisera arkivet så att rätten att ta del av allmänna handlingar underlättas samt skydda arkivet mot förstörelse, skada, tillgrepp och obehörig åtkomst. I skydd mot förstörelse ingår såväl krav på tillgänglighet som att ingen obehörigen ändrar i en arkiverad handling. Kravet på skydd mot obehörig åtkomst tar sikte på skyddsmålet konfidentialitet. Arkivmaterial kan bestå av en mängd olika uppgifter vilket innebär att **hela skalan** av konsekvensnivåer måste kunna tillämpas på de arkiverade informationstillgångarna vad gäller samtliga skyddsmål.

## Verksamhetsperspektivet

Ur ett verksamhetsperspektiv är syftet med informationsklassningen att värdera informationstillgångar med utgångspunkt från deras känslighet och betydelse för organisationen när det gäller konfidentialitet, riktighet och tillgänglighet. Klassificeringen ska göras regelbundet, minst årligen, och vid ändringar av informationstillgångens värde, känslighet och betydelse. Informationsägaren är ansvarig för att detta sker.

Ur ett användarperspektiv ska klassningen ge dem som arbetar med informationen en tydlig indikation på hur den bör hanteras och skyddas. Detta behöver beaktas i behandling av informationen. Standarden ger inte någon ytterligare vägledning och här har vägledningsmaterialet till KLASSA en viktig roll att fylla. Inte minst för att modellen för informationsklassning ska tolkas på ett likartat sätt av SKR:s medlemmar och att likartade informationstillgångar klassificeras på ett likartat sätt och därigenom kan dra fördel av de krav på skyddsåtgärder som KLASSA föreslår. På så sätt kan man undvika situationer där man antingen klassificerar informationen för högt, vilket kan leda till att onödigt kostsamma säkerhetsåtgärder vidtas, eller att man klassificerar informationen för lågt, vilket istället kan innebära risker för verksamhetens förmåga att nå sina mål. Ett exempel på detta skulle kunna vara att informationen inte är tillgänglig i den utsträckning som behövs, genom att aspekten

# Processorienterad informationskartläggning

Mot bakgrund av att informationshanteringen blir allt mer komplex och att informationsklassningen utgår från en given informationsmängd är det av yttersta vikt att skapa en förståelse för i vilka sammanhang information uppstår, hanteras, lagras, bearbetas osv. Inte sällan förekommer samma informationsmängd i olika sammanhang och det kan få stor påverkan på informationsklassningens kvalitet om det inte är känt.

Den processorienterade informationskartläggningen kan också vara en hjälpande hand för att förstå ägandeskapet till en viss informationsmängd i enlighet med resonemanget i det tidigare avsnittet om informationsklassning.

### Allmänt om informationsförvaltning

Hanteringen av verksamhetsinformation i enlighet med ISO 15489 är en tänkbar grund för ett ledningssystem för verksamhetsinformation (LVI), som definieras i ISO 30300-serien. Ett LVI kopplar ihop hanteringen av verksamhetsinformation med organisationens framgång och ansvar genom att etablera ett ramverk bestående av riktlinjer, mål och direktiv för verksamhetsinformation. Det fastställer följande krav:

- fastställda roller och ansvar,
- systematiska processer,
- övervakning och utvärdering,
- granskning och förbättring.

För den tänkta målgruppen är en viktig del att också förhålla sig till standarden SS-EN ISO 19650 som beskriver principer för hantering av anläggningsinformation över hela tillgångens livslängd.

Denna rapport för inte något djupare resonemang kring informationsförvaltning eller informationshantering utan har ett huvudsakligt fokus på informationssäkerhet men nämner detta kort eftersom det finns en tydlig beröringspunkt.

### Modell och metodik

Informationsklassningen är tämligen standardiserad och har ett tydligt ramverk att förhålla sig till som SS-ISO/IEC 27001 och 27002. Metodiken för en processorienterad informationskartläggning (POIK) har inte lika fasta ramar och också fler beroenden varför det snarare ska ses som ett tillvägagångssätt.

Myndigheten för samhällsskydd och beredskap (MSB) och Riksarkivet (RA) genomförde ett initiativ 2012 under rubriken Vägledning för processorienterad informationskartläggning[15] som är en bra och ganska enkel vägledning att förhålla sig till. Fördelen med att vägledningen är enkel är att tillämpligheten ökar vilket inte ska underskattas då vi fokuserar på strömmande data.

## Verksamhetsprocesser och informationshantering

Ansatsen för den processorienterade informationskartläggningen kan sammanfattas i tre lager:

- Verksamhetslagret, som exempelvis beskrivs genom att följa en process
- Informationslagret, som beskriver de informationsmängder som:
    - Skapas
    - Hämtas
    - Bearbetas
    - Lagras
- Informationsbärlager, som beskriver informationsbärare

Sammanfattningsvis kan sägas att en process har relation till en eller flera informationsmängder som i sin tur bärs av ett antal informationsbärare.

Det synsättet är relativt enkelt att applicera på strömmande data där man kan se en process som styr värme eller kyla i en fastighet med ett antal informations-mängder som grund, exempelvis inom- och utomhustemperatur. Det gör att den processorienterade informationskartläggningen enkelt kan användas för att identifiera informationsmängder, informationsägare och de förväntade kraven på informationsmängderna.

[15] Vägledning för processorienterad informationskartläggning (https://rib.msb.se/filer/pdf/26410.pdf)

Ur ett informationsklassningsperspektiv är det enkelt att ställa sig frågan kopplat till exemplet ovan:

Konfidentialitet – Vad blir skadan om informationen hamnar i orätta händer?

- Om inom- eller utomhustemperatur som används för att styra värme eller kyla i en byggnad tillgängliggörs blir skadan sannolikt **försumbar (0)**

Riktighet – Vad blir skadan om informationen inte är korrekt?

- Om inom- eller utomhustemperatur som används för att styra värme eller kyla i en fastighet inte är korrekt blir skadan sannolikt **måttlig (1)** eller **betydande (2)**

Tillgänglighet – Vad blir skadan om informationen inte är tillgänglig?

- Om inom- eller utomhustemperatur som används för att styra värme eller kyla i en fastighet inte är tillgänglig blir skadan sannolikt **måttlig (1)** eller **betydande (2)**

Värderingen av skadan beror givetvis på hur lång tid det går från att informationen inte är korrekt eller otillgänglig, liksom på hur stor avvikelsen är och vad omgivningstemperaturen är vid det aktuella tillfället.

Om informationen inte hade satts in i sitt rätta sammanhang hade det varit svårt att värdera en informationsmängd som inom- och utomhustemperatur. De aktuella informationsmängderna kan ha fler beroenden som gör att klassificeringen blir annorlunda.

Ackumulerade och aggregerade informationsmängder beskrivs närmare i ett eget avsnitt.

## Rätt bemanning

I metodiken för processorienterad informationskartläggning är utgångspunkten verksamhetsprocesserna. Exempel på lätt igenkända verksamhetsprocesser är anskaffning och rekrytering. Ur perspektivet strömmande data är processerna inte lika lätt igenkända för gemene man, men för den som vet hur exempelvis värme eller kyla styrs i en fastighet är det uppenbart. Det är därför av största

värde att arbetet med kartläggningen görs med rätt personer i rummet vilket också poängteras i MSB/RA:s vägledning.

## Verktygsstöd

Det finns ytterligare ett stödverktyg, KLASSA verksamhetsinformation eller Arkiv-KLASSA, ibland också benämnt Informations-KLASSA[16] för att inte sammanblandas med KLASSA för informationssäkerhet eller Informations-säkerhets-KLASSA. Det är ett verktyg från Samrådsgruppen för kommunala arkivfrågor[17] där SKR ingår.

Ett av huvudsyftena med Informations-KLASSA var att utarbeta en hierarkiskt uppbyggd klassificeringsstruktur för verksamheter i kommuner och regioner. Strukturen är beskriven och systematiserad till ett punktnoterat schema. Schemat kan sedan användas som underlag för en diarieplan men även nyttjas till dokumentmetadata, struktur för e-arkivet etc.

Klassificeringsschemat är uppdelat i tre delar:

- Ledning[18]
- Verksamhetsstöd[19]
- Kärnverksamhet[20]

I schemat som avser verksamhetsstöd går det exempelvis att finna notation 2.6.1.1 som avser processen att uppföra lokal.

Inom ramen för detta initiativ har det diskuterats om det finns behov av ett liknande systematiserat schema för att beskriva processer inom ramen för exempelvis fastighetsautomation. Uppfattningen är att det är svårt att i nuläget se värdet av ett sådant schema, men att det bör bevakas och om behovet uppstår ska det harmoniseras med här nämnda klassificeringsschema.

---

[16] Informations-KLASSA (http://samradsgruppen.se/index.php/rad-och-stod)
[17] Samrådsgruppen för kommunala arkivfrågor (http://www.samradsgruppen.se/)
[18] Klassificering Ledning (http://www.arkivkonsultab.se/wp-content/uploads/5.Klassa/VT1-VT3/VT-1-LEDN-KLASSA-2.1.xlsx)
[19] Klassificering Verksamhetsstöd (http://www.arkivkonsultab.se/wp-content/uploads/5.Klassa/VT1-VT3/VT-2-ST%C3%96D-KLASSA-2.1.xlsx)
[20] Klassificering Kärnverksamhet (http://www.arkivkonsultab.se/wp-content/uploads/5.Klassa/VT1-VT3/VT-3-K%C3%84RN-KLASSA-2.1.xlsx)

SKR ser att dessa båda verktyg, som utvecklats parallellt under lång tid för olika syften också har väldigt tydliga beröringspunkter. I releaseplanen för Informationssäkerhets-KLASSAv4 finns en ambition att stödja den process-orienterade informationskartläggningen och klassificeringsschemat för att därigenom fånga upp Informations-KLASSA:s egenskaper i ett och samma verktyg. Bedömningen i skrivande stund är att det kan ske sent 2022 eller 2023.

## Exemplet Region Gävleborg

Region Gävleborg har genomfört en processorienterad informationskart-läggning över hela regionen som en del i ett större pågående arbete med att utveckla informationsförvaltning inom regionen.

Regionen har tagit avstamp i MSB/RA:s vägledning och Informations-KLASSA:s klassificeringsstruktur med vissa anpassningar. Metodiken har sedan vidareutvecklats för att inkludera perspektiven:

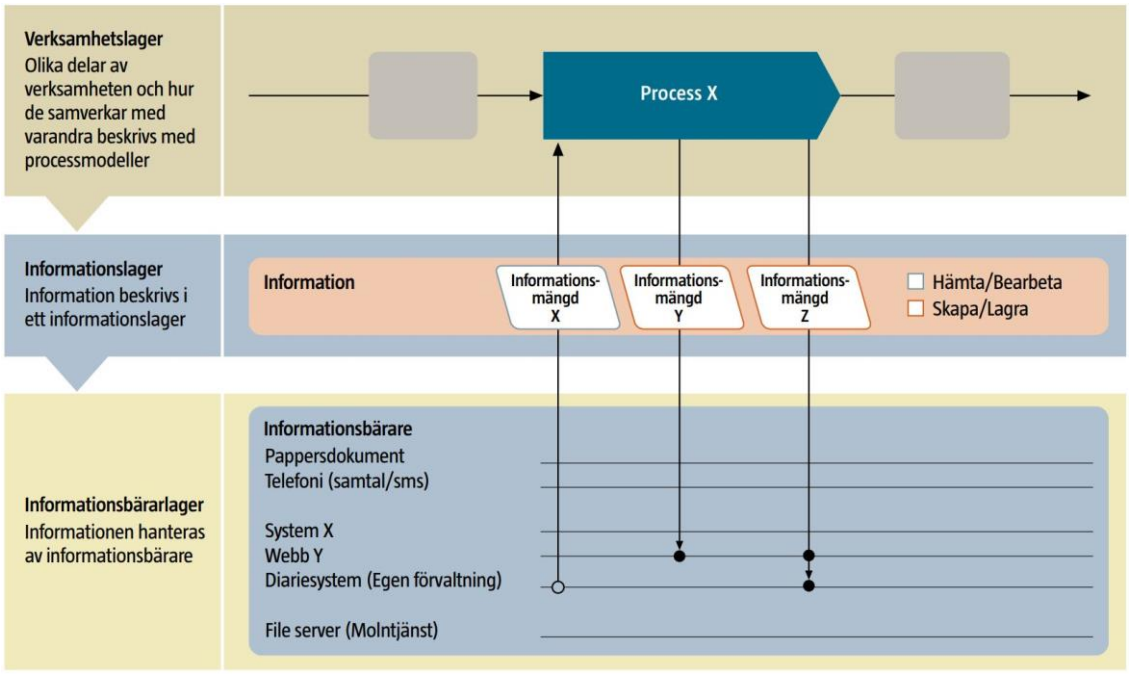
- registratur
- informationssäkerhet
- dataskydd
- regionarkiv

Funktionerna har ett gemensamt mål, det vill säga att ha en god överblick över den information som finns och att informationens konfidentialitet, riktighet och tillgänglighet garanteras och skyddas. Det är en utmaning att tillgodose den egna verksamhetens och omvärldens behov av informationsförsörjning, och samtidigt vidmakthålla den enskildes rättigheter och integritet. Detta kan i vissa fall vara motstridiga intressen.

Arbetet är genomfört med ett huvudsakligt fokus på en regions administrativa processer. Mot bakgrund av att denna vägledning i huvudsak har fokus på strömmande data ska detta ses som en inspiration för att strukturera den informationen på ett motsvarande sätt.

Det är dock viktigt att poängtera att varje verksamhet har behov av att göra motsvarande kartläggning vilket inte nog kan understrykas. Inte minst mot bakgrund av att merparten av den offentliga organisationens verksamhets-information utgör allmänna handlingar vilket förutsätter en god informations-förvaltning, och en god informationsförsörjning förutsätter att både information och informationsbärare som hanteras i organisationen är identifierade.

**Figur 4. Översiktlig bild över vägledningens tre lager – ur MSB Vägledning för processorienterad informationskartläggning**




Källa: MSB[21]

Ritningen blir ett bra diskussionsunderlag för det fortsatta analysarbetet då det skapar en tydlighet och alla deltagare får samma bild att referera till.

Kopplat till detta görs också en dokumentation av processen som beskriver informationsägare, typ av handling, gallring, arkivering, sekretess (referens till OSL), förekomst av personuppgifter osv. Tillvägagångssättet innebär också att regionen ser i vilka sammanhang en och samma informationsmängd förekommer vilket underlättar informationsklassning. Det blir också tydligt vad breda informationsbärare, exempelvis e-post, får för aggregerad informationsklassning. Just exemplet e-post, där det sannolikt finns en begränsning för vilka skyddsåtgärder som kan påföras, kan inte bära information med exempelvis konfidentialitet högre än **måttlig (1)**.

Om metodiken tillämpas rätt kan informationsbärare som inte lämpar sig för en viss informationsmängd identifieras och hanteras. Sammantaget innebär

[21] Vägledning för processorienterad informationskartläggning (https://rib.msb.se/filer/pdf/26410.pdf)

metodiken inte bara att det vardagliga informationssäkerhetsarbetet förbättras då metodiken syftar till att naturligt väva in arbetet i verksamheten, det ger också indirekta effekter där olämpliga tillvägagångssätt kan identifieras och hanteras som i exemplet ovan.

Även om Region Gävleborg inte fokuserat på strömmande data är det tydligt vilka positiva effekter det processorienterade informationskartläggningsarbetet ger. I ett efterföljande avsnitt ges exempel på hur det kan appliceras på strömmande data.

# Aggregerade och ackumulerade informationsmängder

## Begrepp och förtydliganden

En **informationsmängd** är en gruppering av information, exempelvis i form av ett dokument, en databas eller liknande. En informationsmängd innehåller en eller flera informationstyper. En informationsmängd utgör minsta möjliga meningsfulla del, till exempel ska en PDF inte delas upp i dess olika informationstyper utan ses som en informationsmängd. Ett klassificeringsobjekt innehåller normalt ett flertal informationsmängder.

En **informationstyp** är information av ett visst slag. Man kan välja att definiera en informationstyp som en informationsmängd och klassificera den. Om och vilka informationstyper en organisation väljer att definiera som en informationsmängd och klassificera beror på organisationens behov. Att identifiera viktiga informationstyper kan underlätta klassificeringen, till exempel när en viss typ av information är spridd i stora delar av organisationen, såsom personuppgifter, eller är av särskild betydelse för organisationen. Exempel på informationstyper som kan vara av särskild betydelse är kundregister, ekonomisk redovisning, riskanalyser, källkod, ritningar, forskningsresultat eller liknande beroende på vilken verksamhet som bedrivs. Informationstyper som finns på många ställen i en organisation eller som är särskilt viktiga för hela organisationen kan klassificeras organisationsgemensamt, för att undvika att olika verksamheter lägger tid på att klassificera samma informationstyp flera gånger.[22]

Aggregerade uppgifter betyder att flertalet olika typer av uppgifter samlas och tillsammans utgör ett nytt skyddsvärde, medan ackumulerade uppgifter betyder en ökad volym av samma typ av uppgifter. Om enskilda uppgifter som saknar säkerhetsskyddsklass eller är indelade i en av säkerhetsskyddsklasserna begränsat hemlig, konfidentiell eller hemlig samlas, kan det i vissa fall medföra att en högre säkerhetsskyddsklass ska tillämpas. Så är fallet om den aggregerade

[22] MSB:s metodstöd

eller ackumulerade informationen gör att en antagonist kan dra andra, helt nya slutsatser av uppgiftssamlingen än av varje enskild uppgift[23], exempelvis:

- Stora mängder information lagras i systemet (ackumulering).
- Flera olika informationsmängder som när de sammanförs skapar känsligare information vilket innebär ett högre skyddsbehov (aggregering).
- En informationstyp är ett visst slag av information. En informationstyp kan finnas lokalt i en verksamhet eller vara spridd över hela organisationen, som exempelvis personuppgifter. Informationstyper som finns på många ställen i en organisation kan gärna klassificeras centralt, för att undvika att olika verksamheter klassificerar samma informationstyp på olika sätt.

### Exempel på aggregerade informationsmängder

Med aggregerade data menas att olika informationstyper förs samman och bildar en informationsmängd, t.ex. ett dokument eller viss handling, och att konsekvenser och skyddsbehov blir större än för de ingående informations-typerna var för sig vilket resulterar i en högre informationsklassning.

Ett annat exempel är om en användare kombinerar uppgifter om fastigheter och anläggningar, infrastruktur, tekniska system och noder, material, förmågor och personalresurser.

### Klassning av aggregerade informationsmängder

Exempel: System med positionering av renhållningsfordon och avfalls-containrar

I den här IoT-tillämpningen används GPS-data för att främst positionsbestämma olika typer av avfallscontainrar och skicka denna information till ytterligare ett system för koordinering av utlåning och upphämtning av containrarna. Med hjälp av systemet kan man exempelvis inventera antal containrar inom ett avgränsat geografiskt område, bevaka att containrar inte förflyttas ut ur ett geografiskt område utan tillstånd samt identifiera exakta koordinater vid upphämtning.

[23] 4 kap. 6 § Säkerhetspolisens föreskrifter (PMFS 2019:2) om säkerhetsskydd

### Vägledning avseende klassificeringsnivå – Konfidentialitet

Vid klassning av konfidentialiteten är det viktigt att beakta den aggregerade informationen och inte endast de specifika koordinater som IoT-sensorn skickar vidare. I systemet kombineras GPS-data i form av koordinater med kund-information som namn, organisationsnummer, adresser samt fotografier av platser för återrapportering. Med hänsyn till att systemet innehåller person-uppgifter är en rimlig klassificeringsnivå **betydande (2)**.

### Vägledning avseende klassificeringsnivå – Riktighet

Informationen i allmänhet och GPS-data i synnerhet bör kunna klassificeras som **betydande (2)** med hänsyn till Riktighet. Informationen behöver vara korrekt för att containrar ska kunna hämtas och hanteras på rätt sätt och felaktig information leder till merarbete och högre kostnader. Därutöver kan organisationens eller kommunens förtroende skadas och om avfallscontainrar innehåller miljöfarligt avfall finns risk för att det inte tas om hand i tid.

### Vägledning avseende klassificeringsnivå – Tillgänglighet

Även om tillgängligheten till systemet i allmänhet och information om GPS-data och containrars koordinater i synnerhet inte är direkt avgörande för att organisationen ska kunna genomföra sin verksamhet så förlitar man sig på att informationen är tillgänglig i hög grad. Skulle systemet och informationen vara otillgänglig i mer än 24 timmar klassificeras tillgänglighetsaspekten som **betydande (2)**. Detta på grund av att effektiviteten märkbart går ner samt att kostnaderna ökar.

## Exempel på ackumulerade informationsmängder

Ackumulerad data innebär att flera förekomster av samma informationstyp eller informationsmängd samlas och lagras på samma ställe, t.ex. i ett arkiv eller en databas vilket ofta leder till ökat skyddsbehov.

Ett exempel på att information samlas är om en användare sparar adress-uppgifter över tid så att flyttmönster framträder.

## Klassning av ackumulerade informationsmängder

**Exempel: Fastighets- och befolkningsplattformen är en plattform för grunddata om fastighets- och befolkningsinformation.**

FB hanterar fastighets-, byggnads- och lägenhetsinformation från Lantmäteriet samt folkbokföringsinformation från Skatteverket i en och samma databas. Databasen är spatial och hanterar, förutom registerdata från Lantmäteriet och Skatteverket, också ”kartobjekten” fastighetsyta, byggnadsyta och område. Informationen kan nås genom webbklient eller genom verksamhets- och/eller kartsystem som integreras med plattformen via dess öppna gränssnitt.

Informationsklassningsnivå för konfidentialitet hamnar på **allvarlig skada (3)** för enskilda individer ifall information om skyddade identiteter röjs. Inga personer med skyddad folkbokföring syns i systemets officiella vyer. Den höga risken ligger i om data och kunskaper kopplas samman till en slutsats som röjer skyddade personer. Även mängden personuppgifter i databasen påverkar informationsklassningsnivån.

Riktigheten klassificeras på nivå **måttlig skada (1)** och bedöms lägre än för konfidentialitet på grund av att följderna enbart blir något mer administrativt arbete och därför något längre handledningstider i andra processer. Kontroll-funktioner, främst i form av att många tittar på informationen, och att den är så pass beroende av att vara korrekt innebär att riktigheten och eventuella felaktigheter kan identifieras snabbt och i flera led. Felaktigheter kan få vissa ekonomiska följder för verksamheter.

Nivå för tillgänglighet bedöms till **måttlig skada (1)** eftersom den enda följden som är uppenbar vid en otillgänglig tjänst är förlängda handledningstider i relaterade processer, vilket medför administrativt arbete.

## Informationsklassning

I exemplet med AI-baserad fastighetsautomation gäller det att förstå vilka krav som den aktuella byggnaden är förenad med och vilka de icke-önskvärda scenarierna är. Det förstnämnda översätts till krav på informationssäkerhet med informationsklassning som grund och det senare är resultatet av en sedvanlig riskanalys.

I avsnittet om processorienterad informationskartläggning fördes resonemanget ur ett informationsklassningsperspektiv kopplat till styrning av värme/kyla i en fastighet:

Konfidentialitet – Vad blir skadan om informationen hamnar i orätta händer?

- Om inom- eller utomhustemperatur som används för att styra värme eller kyla i en fastighet tillgängliggörs blir skadan sannolikt **försumbar (0)**

Riktighet – Vad blir skadan om informationen inte är korrekt?

- Om inom- eller utomhustemperatur som används för att styra värme eller kyla i en fastighet inte är korrekt blir skadan sannolikt **måttlig (1)** eller **betydande (2)**

Tillgänglighet – Vad blir skadan om informationen inte är tillgänglig?

- Om inom- eller utomhustemperatur som används för att styra värme eller kyla i en fastighet inte är tillgänglig blir skadan sannolikt **måttlig (1)** eller **betydande (2)**

I resonemanget är det tydligt att det i första hand är krav på riktighet och tillgänglighet som återfinns i den här typen av tillämpningar. I SKR:s rapport KLASSA för IoT som fokuserade på olika typer av IoT-tillämpningar var mönstret detsamma.

Det finns tillfällen när även den information som samlas in kan ha en hög grad av konfidentialitet men det har sällan en stark koppling till förmåga att styra och reglera något, utan det kravet kan exempelvis drivas av ovilja att dela viss mätdata som kan skapa badwill.

I det aktuella exemplet har riskanalyser genomförts och normalt har den typen av information höga krav på konfidentialitet varför vi inte delar dem i denna rapport, men vi kan utan att röja någon skyddsvärd information redovisa hur olika risker har mitigerats:

- Det AI-baserade fastighetsautomationssystemet kan helt kopplas ur på mindre än 5 minuter.
- Den ursprungliga styrningen används som fall-back.
- Det AI-baserade fastighetsautomationssystemet kan aktiveras/deaktiveras såväl manuellt som automatiskt vid avvikelser.

I det aktuella exemplet innebär dessa mitigerade åtgärder att vid förlorad riktighet eller tillgänglighet till de informationsmängder som förser det AI-baserade fastighetsautomationssystemet med beslutsunderlag är påverkan **måttlig (1)** avseende riktighet och tillgänglighet under förutsättning att de föreslagna åtgärderna för mitigering är effektiva.

## Processorienterad informationskartläggning

I det aktuella exemplet har ingen processorienterad informationskartläggning genomförts. Detta beror till viss del på att processen är ny och en stor del av informationsmängderna, exempelvis de 20 000 sensorerna, inte förekommer i andra sammanhang. Det gör den initiala bilden tämligen homogen. Sannolikt kommer komplexiteten att öka över tid och informationsförsörjningen av det AI-baserade fastighetsautomationssystemet att breddas varför det kan vara på sin plats att göra en processorienterad informationskartläggning för att trygga informationssäkerheten över tid i lösningen och annan tillämpning som berörs.

## Aggregerade och ackumulerade informationsmängder

Det är uppenbart att det aktuella exemplet också är ett exempel på aggregerade och ackumulerade informationsmängder. En ensam informationsmängd som föder det AI-baserade fastighetsautomationssystemet har ringa värde, men den sammanlagda bilden av den information som behandlas har såväl ett högt ackumulerat värde som ett högt aggregerat värde. Detta gör att kraven på konfidentialitet för den information som föder det AI-baserade fastighets-automationssystemet ökar.

I de tidigare resonemangen bedömdes kraven för konfidentialitet som **försumbara (0)** men mot bakgrund av den samlade bilden av den information

som behandlas ökade kraven. Under förutsättning att ingen av de insamlade informationsmängderna berörs av de regulatoriska kraven som belysts i denna rapport kan konsekvensnivån antas vara **måttlig (1)**. Om kraven gäller är konsekvensnivån för konfidentialitet sannolikt **betydande (2)** eller **allvarlig (3)** beroende på vilka regulatoriska krav som blir aktuella.

## Skyddsåtgärder enligt KLASSA

Den summerade bedömningen av det AI-baserade fastighetssystemet i det här exemplet där konfidentialitet, efter resonemanget om ackumulerade och aggregerade informationsmängder, är **måttlig (1)** och där riktighet och tillgänglighet är **måttlig (1),** gäller under förutsättningen att det AI-baserade fastighetsautomationssystemet installerats som beskrivs här.

I bilaga 2 finns utfallet med krav på en informationstillgång som har klassificerats på konsekvensnivån **måttlig (1)** för samtliga säkerhetsaspekter.

## Övriga reflektioner

Givet det resonemang som förts i detta exempel kring mitigerande åtgärder för identifierade risker utgör det AI-baserade fastighetssystemet i sin nuvarande form inte någon större risk med avseende på själva fastighetsautomationen, förutsatt att åtgärderna är effektiva.

Det utesluter inte att ett införande kan medföra risk för andra informations-tillgångar. Den infrastruktur som byggs upp för att samla in all tänkbar information kan utgöra en risk. Inte nödvändigtvis mot fastighetsautomationen, men det finns exempel, inte relaterat till SISAB:s implementation, där en organisations it-infrastruktur är tämligen öppen och inkluderande vilket har lett till att organisationens mest skyddsvärda tillgångar är åtkomliga från en obevakad sensoranslutning.

I bilaga 1 beskrivs ett arbete som Svenska Stadsnätsföreningen (SSNF) och SKR bedrivit tillsammans som bland annat adresserar det faktum att även infrastrukturen måste dimensioneras för såväl nya som befintliga hotbilder.

# Bilaga 1 – ”Säkerhetsspåret”

## Bakgrund

Samhällets beroende av tjänster baserade på lösningar, utrustningar och system för Internet of Things (IoT) ökar i en allt snabbare takt. IoT finns i många delar av samhället: i hemmet, i offentlig verksamhet och inom industrin. Beroendet av IoT gör att hanteringen av utrustning och system för IoT, och den infrastruktur som de kopplas upp till, måste vara tillförlitlig och säker. Detta gäller även tillverkningen av utrustning samt leveranskedjan till slutanvändaren.[25]

Internet of Things (IoT), eller sakernas internet, för med sig stora möjligheter men innebär också risker. Dessa risker behöver tydliggöras för att kunna identifiera relevanta åtgärder.

## Effektmål

- En generisk metod för att införa IoT-lösningar som anknyter till framtagna vägledningar. Den generiska metoden ger förutsättningar för kommuner och regioner att enklare använda KLASSA.
- Vägledningen kommer att innehålla beskrivna arbetssätt och visuella processer som utgör stöd vid införande av IoT-tjänster inom kommunal och regional förvaltningsverksamhet (kopplad till Upphandlingsmyndighetens och/eller SKR:s försörjningsplan).
- Rätt nivå av säkerhet i IoT-tjänster genom möjlighet att simulera den nya tjänsten samt korrigering av tjänsten innan man väljer att gå vidare. Stöd för detta ges i vägledningen tillsammans med verktyget KLASSA.

[25] Vägledning för robust och säker IoT (https://www.ssnf.org/globalassets/nat-i-varldsklass/rdi/iot/rdi_vagledning_robust__saker_iot_v1_0.pdf)

## Projektmål och leverabler

- En generisk process för hur man tar fram ett underlag inför en självskattning via stödverktyget KLASSA.
- Beskrivningar, samt eventuella mallar/checklistor kopplade till processen (beskrivningar etc. tas fram av rätt kompetens i projektet).
- Processen/metoden exemplifierad utifrån persona/scenarion, som är hämtade från deltagande kommuner.
- Processen/metoden ska vara så generisk att den kan användas av en kommun eller region som ska ta fram underlag inför en självskattning via KLASSA för en IoT-tjänst.

## Kartlägga nuläget

För att kunna genomföra en förändring som svarar mot de verkliga behoven, behöver en kartläggning av behov som beskriver nuläge och marknad göras. Det är viktigt att väl avvägda resurser anslås till den här fasen. Det kan vara lätt att fastna i kartläggningen och aldrig komma vidare till följande faser men om för lite resurser läggs ner på kartläggningen riskerar följande faser att vila på osäker grund.

**Råd**: Gör ett väl genomlyst och avvägt val av hur stora resurser som kartläggningen ska tilldelas.

**Rekommendation**: Gör ett strategiskt val av vilka kompetenser och aktiviteter som kan komma att behövas för att kartlägga behovsbilden och säkra användbarheten.

### Exempel: Robust och säker tillgång till internet

För att offentlig sektor ska klara av det ökande trycket med allt fler invånare som har behov av hjälp, behövs alternativ till insatser som idag kräver personella resurser. Att invånare ska känna trygghet och självständighet i vardagen bör vara grundläggande. För att underlätta finns det tjänster inom välfärdstekniken; exempelvis digital tillsyn, digitala trygghetslarm, larmmattor, dörrlarm med mera som kan hjälpa användaren att leva ett självständigt liv på egna villkor. Gemensamt för välfärdstjänster är behovet av tillgång till internet. Här presenteras två scenarier som belyser vanliga frågor som kan uppstå vid införande av välfärdstjänst och åtkomst till internet, både i ordinärt boende och verksamhetens lokaler.

### Uppkoppling av välfärdsteknik i ordinärt boende

Kommunen erbjuder välfärdstekniktjänster som ett komplement till fysiska besök av hemtjänsten för att möta brukarnas behov av trygghet och självständighet. Att använda nya tjänster för att komplettera omsorgen kan rätt implementerat, utöver att höja kvaliteten, också innebära ekonomiska, miljömässiga och tidsmässiga vinster. Allteftersom brukarna får utökade behov så erbjuds fler välfärdstekniktjänster, vilket kan innebära att antalet produkter hemma hos kunden ökar.

En av utmaningarna för kommunen är att ta ställning till hur dessa välfärdstjänster ska erbjudas och framförallt hur åtkomst till internet ska lösas för olika tjänster.

För vissa tjänster räcker det med full funktion vid behov, för andra som till exempel vid hemmonitorering av olika hälsotillstånd ställs högre krav på både tillgänglighet och tillförlitlighet. Vissa tjänster klarar sig med 2G medan andra kräver betydligt högre bandbredd och kvalitet i tjänsten.

### Hur kan kommunen tänka kring uppkopplingsmöjligheter för välfärdstekniktjänster?

De flesta leverantörer av välfärdstekniktjänster erbjuder en ”komplett lösning”; dvs. en produkt, bakomliggande mjukvara, internetåtkomst via exempelvis SIM-kort och support, som paketeras som tjänst och erbjuds till kommunen via hyresavtal. Denna lösning gör det enkelt för kommunen att bara ha en leverantör som ansvarar för hela kedjan i välfärdstekniklösningen med support och felsökning.

En nackdel med detta upplägg är att kommunen kan få flera olika leverantörer när antalet tjänster ökar. Varje leverantör har sin egen lösning med uppkoppling och så kallad hubb. Många leverantörer är inte villiga att dela uppkopplingsmöjligheter med sina konkurrenter. Kommunen blir ”tvingad” att köpa flera tjänster från en och samma leverantör för att kunna samutnyttja uppkopplingsmöjligheter, alternativt bekosta flera abonnemang för tjänster från olika leverantörer.

Andra alternativ som diskuterats i omgångar är om kommunen och kunden kan dela på ansvar och kostnad för uppkoppling. Exempelvis att kunden står för internetåtkomst och att kommunen står för produkten, alternativt att kommunen bara levererar digitala tjänster om tillgång till fiber finns.

### Vad säger juridiken?

Utgångspunkten i socialtjänstlagen är att kunden ansöker om en insats (bistånd). Kunden beviljas insatsen, till exempel tillsyn eller trygghetslarm, om det är nödvändigt för att kunden ska ha en skälig levnadsnivå och behovet inte kan tillgodoses på annat sätt. Kommunen har ansvar för att verkställa ett beviljat biståndsbeslut och bedömer hur beslutet ska verkställas. Den enskilde kan alltså inte kräva att en insats ska utföras på ett visst sätt. Det innebär att kommunen kan bestämma att till exempel tillsyn på natten sker digitalt istället för att personal åker hem till den enskilde.

Det är inte möjligt att villkora en insats med att den enskilde har en egen uppkoppling, eller att den eventuella uppkoppling som finns har tillräcklig kvalitet eller hastighet. Om kunden har en egen uppkoppling som används kommer kommunen ändå vara ansvarig för att en insats kan verkställas, till exempel att tillsynen eller larmet fungerar. Det är viktigt att kommunen får indikation på om tjänsten inte fungerar, så att alternativa åtgärder kan sättas in, exempelvis att personal ringer eller gör fysisk tillsyn när tekniken inte fungerar.

Ska en digital tjänst erbjudas kunden och uppkopplingsmöjligheter inte finns, så behöver kommunen ordna en uppkoppling till kunden inom ramen för beslutets verkställighet. Då detta ligger inom ramen för den beviljade insatsen är det förenligt med likställighetsprincipen i kommunallagen. Finns det inte förutsättningar för uppkoppling där den enskilde bor behöver kommunen verkställa beslutet på annat sätt, till exempel med fysisk tillsyn.

### Råd

- Ta fram en gränsdragningsöverenskommelse för ansvarsfördelning mellan leverantörerna om en tjänst slutar fungera. Det blir extra viktigt om flera leverantörer är inblandade i leveransen av tjänster. Är det kommunen, leverantören eller telebolaget som ansvarar för till exempel felsökning och information?
- Kommunen bör göra ett aktivt ställningstagande i sitt erbjudande av välfärdsteknikstjänster som kräver uppkoppling. Vilken typ av uppkoppling som gäller och vad som sker om möjlighet till uppkoppling inte finns. Hur ska alternativ tjänst se ut för att fylla kundens behov?

### Internetuppkoppling till kund i verksamhetens lokaler

Tillgång till internet har blivit en grundläggande förutsättning i det digitala samhället. En kund som flyttar in i särskilt boende är inget undantag. Möjligheter för åtkomst till internet ska finnas på alla boenden, men det kan vara i form av mobilt bredband, andra abonnemang eller del av kommunens nätverk.

Den digitala utvecklingen är eftersatt på en stor del av särskilda boenden runt om i Sverige och många kommuner brottas med uppkopplingsutmaningar i samband med både nybyggnation och ombyggnation. Det finns behov av samsyn kring bland annat frågeställningen om internetuppkoppling ska erbjudas för både verksamhetens och kundens behov eller enbart till personalen.

Fler och fler kunder i kommunen har smarta telefoner och annan utrustning som de vill kunna fortsätta använda efter att de flyttar till särskilt boende, vilket betyder att efterfrågan på trådlös internetåtkomst ökar.

### Hur kan kommunen tänka avseende tillgång till internet för kunden i särskilt boende?

Kommunen behöver ta ställning till om internetuppkoppling ska erbjudas via kommunens eget nätverk och om det i så fall ska ingå i hyran av lägenhet på boendet. Om internetuppkoppling ingår i hyresavtalet bör kommunen ansvara för att tillhandahålla en fungerande support, som är lämplig för kundens behov. Detta med tanke på att kund som får ett särskilt boende beviljat, ofta har behov av ytterligare stöd och support än enbart omvårdnad.

I en övergångsperiod kan en utökad kostnad för internetåtkomst bli ett ovälkommet tillägg för de som inte behöver åtkomst till internet. Särskilt kännbart blir det för de befintliga hyresgästerna vid tillfället då förändringen genomförs. Överväg övergångsrutiner för de befintliga hyresgästerna. Om kostnaden är en kvalitetshöjning kan den inte påtvingas befintliga hyresgäster.

Kommunen behöver även ta ställning till i hur stor utsträckning internettjänsten är tillgänglig. Hur hanteras eventuella avbrott och belastning i nätverket? Ska till exempel kundens nätverksuppkoppling kunna strypas till fördel för verksamhetskritiska system?

Om kunden själv står för internetuppkopplingen är det viktigt att på förhand komma överens med kunden hur denne ska hantera support och felanmälan på

den egna utrustningen. Även i detta fall behöver kommunen ta ställning till i vilken omfattning omvårdnadspersonalen kan hjälpa kunden med eventuell felsökning och support.

### Vad säger juridiken?

#### Råd

- Det är numera förhållandevis vanligt att bredband ingår i hyran för många medborgare, detsamma bör kunna gälla när kommunen är hyresvärd. Kommunen bör därför kunna erbjuda åtkomst till internet som en del av den boendes hyra.
- Ta ställning till om internetuppkoppling ska erbjudas hyresgästen som en del av hyran för lägenhet på särskilt boende och hur denna tjänst ska tillhandahållas.
- Ta ställning till om nätverken ska vara separata för kund och verksamhet och i vilken omfattning tillgång till internetuppkoppling sker. Det är viktigt att känslig utrustning och verksamhetskritiska tjänster alltid har tillräckligt med kapacitet för att fungera korrekt.

### Identifiera roller och minimikrav

Aktören definierar vilken typ av IoT-roll/er som är tillämplig samt genomför en ändamålsbaserad bedömning av den säkerhet och integritet som speglar olika säkerhetsnivåer kopplat till systemets/enhetens tillämpning (till exempel blåljus/kris, hemautomatisering).

Se beskrivningar av roller i Robust och säker IoT (Vägledning, Svenska Stadsnätsföreningen).

Minimikraven för den valda rollen analyseras sedan i enlighet med Kravanalys, Robust och säker IoT (Rutin och handledning, Svenska Stadsnätsföreningen).

Aktören upprättar en beskrivning över lösningarna för uppfyllda krav samt upprättar och tidsätter en handlingsplan för att åtgärda avvikelser mellan befintligt läge och minimikraven.

### Identifiera information, dataströmmar och informationsklassificera

Ur ett verksamhetsperspektiv är syftet med informationsklassningen att värdera informationstillgångar med utgångspunkt från deras känslighet och betydelse för organisationen när det gäller konfidentialitet, riktighet och tillgänglighet.

Klassificeringen ska göras regelbundet, minst årligen, och vid ändringar av informationstillgångens värde, känslighet och betydelse. Informationsägaren är ansvarig för att detta sker.

Ur ett användarperspektiv ska klassificeringen ge dem som arbetar med informationen en tydlig indikation på hur den bör hanteras och skyddas. Det behöver beaktas i behandling av informationen. Standarden ger inte någon ytterligare vägledning och här har vägledningsmaterialet till KLASSA en viktig roll att fylla. Inte minst för att modellen för informationsklassning ska tolkas på ett likartat sätt av SKR:s medlemmar och att likartade informationstillgångar klassificeras på ett likartat sätt för att därigenom kunna dra fördel av de krav på skyddsåtgärder som KLASSA föreslår. På så sätt kan man undvika situationer där man antingen klassificerar informationen för högt, vilket kan leda till att onödigt kostsamma säkerhetsåtgärder vidtas, eller att man klassificerar informationen för lågt, vilket istället kan innebära risker för verksamhetens förmåga att nå sina mål. Ett exempel på detta skulle kunna vara att informationen inte är tillgänglig i den utsträckning som behövs, genom att aspekten tillgänglighet värderats för lågt och åtgärder för hög tillgänglighet därför inte implementerats.

Informationsklassning av IoT-tjänster handlar om att

- Identifiera informationstillgångar
- Informationsklassificera dessa informationstillgångar

Se vidare Klassa för IoT, Vägledning från SKR[26]

[26] Klassa för IoT
(https://skr.se/tjanster/merfranskr/rapporterochskrifter/publikationer/klassaforiot.35193.html)

### Upprätta RSA för IoT-system

Genomför en riskanalys och riskbedömning i enlighet med RSA Robust och Säker IoT (Rutin och handledning, Svenska Stadsnätsföreningen).[27]

Observera att verksamhetens art, t.ex. hantering av samhällskritiska funktioner, kan ställa högre krav på säkerhet än de som är angivna som minimikrav i Kravanalys, Robust och Säker IoT (Verktyg, Svenska Stadsnätsföreningen).[28]

[27] Robust och Säker IoT Bilaga 2. Rutin och handledning (https://www.ssnf.org/globalassets/nat-i-varldsklass/rdi/iot/rdi_bilaga_2_rutin_och_handledning_rsa_robust__saker_iot_v1_0.pdf)
[28] Robust och Säker IoT Bilaga 1. Verktyg kravanalys (https://www.ssnf.org/globalassets/nat-i-varldsklass/rdi/iot/rdi_bilaga_1_1_verktyg_kravanalys_robust__saker_iot_v1_0.xlsx)

# Bilaga 2 – Exempel på krav

I exemplet med det AI-baserade fastighetsautomationssystemet fördes ett resonemang som landade i konsekvensnivå **måttlig (1)** för samtliga säkerhetsaspekter givet att det AI-baserade fastighetsautomationssystem implementeras som beskrivs i exemplet.

Med stöd av KLASSA går det med vetskap om att konsekvensnivån är **måttlig (1)** för samtliga säkerhetsaspekter att ta fram SKA-krav för upphandling och ÄR-krav som beskriver ett önskat nuläge utifrån vilket en handlingsplan kan utarbetas.

KLASSAv4 har följande SKA-krav för konsekvensnivå **måttlig (1)** för samtliga säkerhetsaspekter:

**Krav**

- Leverantören ska för sin personal årligen genomföra utbildningar för ökad medvetenhet kring informationssäkerhet.
- Leverantören ska ha rutiner och funktioner för att återlämna beställarens fysiska och elektroniska tillgångar då anställning, uppdrag eller avtal upphör.
- Leverantören ska följa beställarens rutiner och processer för informationsklassning samt tillämpa relevanta säkerhetsåtgärder. Informationsklassningen ska baseras på en riskbedömning som utförs minst vart tredje år.
- Beställarens krav på informationshanteringen ska efterföljas i relation till beställarens informationsklassning. Om sådana krav inte ställts ska leverantören utan anmodan kunna uppvisa de rutiner som gäller hos leverantören för hantering av beställarens tillgångar.
- Leverantören ska tilldela användare hos leverantör och beställare personliga och unika användaridentiteter. Se vägledningen för tillitsnivå 1 (LoA1) för detaljer.
- Leverantören ska följa en överenskommelse för användaråtkomst till beställarens system, tjänster och information. Endast behöriga och enligt överenskommelsen godkända individer ska inneha åtkomst.
- Leverantören ska använda personliga och spårbara användaridentiteter för höga behörigheter som används för systemadministration.

- Leverantören ska på ett säkert sätt distribuera, lagra och återställa autentiseringsinformation (exempelvis lösenord) utan att den kan röjas till obehöriga. Se vägledning för tillitsnivå 1 (LoA1) för detaljer.
- Leverantören ska granska sina användares åtkomsträttigheter minst årligen. Obehöriga eller användare som inte längre behöver åtkomst ska tas bort.
- Leverantören ska ha en rutin för att ta bort användaridentiteter från information, tjänster och system vid avslutande av anställning, avtal eller uppdrag.
- Leverantören ska för sin personal ha fastställda regler för hur autentiseringsinformation ska skyddas och hanteras.
- Leverantören ska ha systemfunktioner för att begränsa åtkomst till information. Endast information eller tjänster som ska vara publika ska kunna nås i system utan godkänd autentisering.
- Leverantören ska tillse att information, tjänster och system kräver autentisering (exempelvis via lösenord). Det ska finnas regler för hur autentiseringsinformation ska hanteras i system och av användaren. Se vägledning för tillitsnivå 1 (LoA1) för detaljer.
- Leverantören ska tillse att fysiska avgränsningar är definierade och tillämpade för skydd av områden med känslig eller kritisk information. Om det avser en datahall eller motsvarande ska leverantören tillse att den uppfyller minst skyddsnivå 1. ("datarum", enligt MSB "Vägledning för fysisk informationssäkerhet i it-utrymmen") eller likvärdigt.
- Leverantören ska ha rutiner som säkerställer att endast behörig personal har fysisk åtkomst till områden med konfidentiell information, exempelvis en datahall.
- Leverantören ska ha funktioner, processer och rutiner för att övervaka och göra prognoser avseende framtida krav på systemprestanda.
- Leverantören ska skydda mot skadlig kod genom att ha säkerhetsåtgärder för att upptäcka, förebygga och återställa de delar som ingår i leveransen.
- Leverantören ska ha rutiner och funktioner för säkerhetskopiering och återställande av information enligt överenskomna tillgänglighetskrav med beställaren. Säkerhetskopior ska skyddas på motsvarande sätt som originalinformationen samt förvaras på en separat plats.

- Leverantören ska tillse att information, tjänster och system har loggningsfunktioner för säkerhetsrelaterade händelser, minst för felaktiga inloggningar, förändring av behörigheter, otillåten anslutning samt överträdelser av behörigheter. Loggning ska ske i samråd med beställaren.
- Leverantören ska skydda loggningsfunktioner och loggningsverktyg mot manipulation och obehörig åtkomst som även omfattar leverantörens personal.
- Leverantören ska tillse att information, tjänster och system, samt relaterad infrastruktur använder tidssynkronisering mot en och samma tidskälla (GPS eller svenska UTC (SP)).
- Leverantören ska bedriva ett kontinuerligt arbete för att identifiera sårbarheter och utan dröjsmål informera en utpekad funktion hos beställaren om denna kan innebära ett hot mot beställarens information, tjänster och system. Upptäckta sårbarheter ska åtgärdas omgående.
- Leverantören ska följa en överenskommelse med beställaren angående krav för informationsöverföring.
- Leverantören ska ha fastlagda och dokumenterade principer och metoder för utveckling av säkra tjänster och system.
- Leverantören ska ha infört säkerhetsåtgärder som skyddar information i programtjänster på publika nätverk mot obehörig åtkomst och obehörig ändring.
- Leverantören ska ha riktlinjer för systemförändringar som avser informationssäkerhet inom sina utvecklingsprocesser.
- Leverantören ska följa beställarens rutiner och processer för åtkomst till organisationens tillgångar.
- Leverantören ska ha rutiner för rapportering, eskalering, hantering av säkerhetshändelser och säkerhetsincidenter. Om incidenten i någon mån påverkar beställaren ska beställaren inkluderas i dessa rutiner.
- Leverantören ska bedöma och besluta ifall en informationssäkerhets-händelse ska klassas som en informationssäkerhetsincident. Om händelsen i någon mån påverkar beställaren ska beställaren inkluderas i detta beslut.
- Leverantören ska ha rutiner för att hantera säkerhetsincidenter enligt gällande lagar och förordningar. Om incidenten i någon mån påverkar beställaren ska en överenskommen och utpekad funktion hos beställaren inkluderas i dessa rutiner.

- Leverantören ska löpande och i samråd med beställaren arbeta för att leveransen i alla lägen följer de aktuella lagar, förordningar, regler och föreskrifter som gäller för beställarens verksamhet.
- Leverantören ska utveckla och införa regler för skydd av personuppgifter med stöd i lagar och förordningar. Dessa regler ska kommuniceras till medarbetare hos leverantören som berörs av leveransen som hanterar personuppgifter.
- Beställaren ska i samråd med leverantören ha rätt att genomföra säkerhetsrevisioner av ingående delar i leveransen.
- Leverantören ska begära tillstånd innan information i system (texter, bilder etc.) eller tjänster återanvänds i andra sammanhang.

# Bilaga 3 – Informationsklassningsexempel

## Mätning av badvattentemperatur

Att mäta temperaturen i badvattnet på kommunala badanläggningar är en konkret och enkel tillämpning av IoT där en service till medborgare blir enklare att förmedla. Sensorerna skickar information trådlöst till en mottagningspunkt på land och vidare därifrån till en nätverksansluten server varifrån organisationen kan läsa och publicera informationen i utvalda kanaler alternativt tillhandahålla informationen via API:er för öppen data. En aspekt att tänka på vid klassning av denna typ av IoT-tillämpning är att moderna sensorer kan samla in mer data och information om vattnet än temperatur. Används sensorer för att mäta fler saker än temperatur kan klassningsnivån för konfidentialitet, riktighet och tillgänglighet mycket väl bli någon annan än vad som föreslås i denna vägledning.

### Vägledning avseende klassningsnivå – Konfidentialitet

Konfidentialiteten hos informationen i denna typ av IoT-tillämpning kan i de allra flesta fall klassas som **försumbar (0)**. Motiveringen till detta är framförallt tvådelad, det är i sig ingen hemlighet vad vattnet har för temperatur vid någon tidpunkt vid kommunala badanläggningar och det är också ett uttalat syfte att sprida denna typ av information med IoT-tillämpningen.

### Vägledning avseende klassningsnivå – Riktighet

Informationen i den beskrivna IoT-tillämpningen kan med hänsyn till riktighet klassas som **måttlig (1)**. Anledningen till att riktighet inte bedöms lägre är att informationen, om den är felaktig när den används, trots allt kan skapa en oangenäm situation och mindre besvär för enskilda individer eller organisationer.

### Vägledning avseende klassningsnivå – Tillgänglighet

Tillgänglighet kan, precis som riktighet, klassas som **måttlig (1)** i denna IoT-tillämpning. Tillgängligheten kan påverkas av olika faktorer, exempelvis kan sensorer skadas eller så kan kommunikationen i andra led störas ut på olika sätt.

Om informationen inte finns tillgänglig kan det således orsaka lindriga besvär för enskilda individer eller organisationer.

## Mätning av grundvattennivåer

I den här tillämpningen används sensorer ute i miljön för att bevaka grundvattennivån inom ett begränsat område. Genom kontinuerlig övervakning av grundvattennivån kan kommunen (eller annan utsedd ansvarig organisation) identifiera när vissa tröskelvärden passeras och underrätta eventuella fastighetsägare om förändringar som skulle kunna medföra negativa konsekvenser. I geografiskt stora områden kan man uppnå stor precision i mätningar över tid till en låg kostnad då behovet av personal som regelbundet besöker flera mätpunkter minskar. Om mätning sker inom ett större område som innefattar flera vattentäkter är det troligt att bedömningen av framförallt konfidentialiteten blir en annan.

### Vägledning avseende klassningsnivå – Konfidentialitet

Den här typen av information som berör grundvattennivåer i ett begränsat område kan klassas som **försumbar (0)** ur ett konfidentialitetsperspektiv. Någon skada bedöms inte kunna uppstå om informationen är allmänt känd, varken av real- eller nära-realtidsdata. Mätarnas koordinater avslöjar mätarnas exakta position men då mätarna i regel är väl synliga, kanske rent av uppmärkta, ute i terrängen bedöms inte den typen av information ändra klassningen. Möjligen skulle information om sensorernas koordinater kunna bidra till skadegörelse men å andra sidan är mätpunkterna skyltade i terrängen.

### Vägledning avseende klassningsnivå – Riktighet

Den information som IoT-sensorerna skapar kan ofta användas som beslutsunderlag för om och vilka eventuella åtgärder som behöver sättas in vid förhöjda grundvattennivåer. Om detta beslutsunderlag är felaktigt skulle det kunna leda till vatten- och sättningsskador på fastigheter inom området. Om fastigheter skadas innebär det dels att enskilda individer kan drabbas av stora besvär samt att organisationen kan bli föremål för skadestånd på uppskattningsvis sexsiffriga belopp, per skadad fastighet. Därutöver tillkommer ett skadat förtroende som kan drabba både enskild organisation eller andra, nära anknutna organisationer exempelvis moder- eller dotterbolag. Därför är en rimlig klassningsnivå **betydande (2)**.

### Vägledning avseende klassningsnivå – Tillgänglighet

Vid beaktande av klassning av tillgänglighet är det bra om det finns en definierad tidshorisont för hur länge information från IoT-sensorer kan accepteras vara otillgängliga. I detta fall får tiden inte överstiga en vecka (168h). Om informationen är otillgänglig längre än så är risken att tröskelvärden passeras som är avgörande för att rätt beslut kan fattas i tid. Konsekvenserna blir i sådana fall likartade som beskrivits för riktighet, **betydande (2)**. Enskilda individer kan drabbas av stora besvär, organisationen kan bli föremål för skadestånd på upp till sexsiffriga belopp och organisationen samt eventuella moder- eller dotterbolag kan drabbas av förtroendeskada.

## Positionering av snöröjningsfordon

I den här IoT-tillämpningen nyttjas GPS-data för att i nära realtid och historiskt redovisa positioner för snöröjningsfordon som genomför renhållningsuppdrag åt kommunen. Dels kan informationen användas av kommunen för uppföljning av upphandlat avtal, dvs. om de uppgifter leverantören är ålagd utförs. Dessutom kan informationen spridas till invånare för att informera om pågående eller avslutade sträckor där renhållning (snöröjning) genomförs.

### Vägledning avseende klassningsnivå – Konfidentialitet

Den information som hanteras i detta system kan med hänsyn till konfidentialitet klassas olika beroende på om det handlar om realtidsdata eller historisk data. I det fall vi bedömer specifikt realtidsdata och om den informationen blev allmänt känd skulle det kunna få **betydande (2)** konsekvenser. Främst i form av att informationen missbrukas i syfte att påverka de individer som genomför själva snöröjningen. Historisk data å andra sidan skulle troligen kunna klassas lägre då det är svårare att missbruka informationen.

### Vägledning avseende klassningsnivå – Riktighet

Informationen som används för att följa upp snöröjningen bör vara så korrekt som möjligt om man väljer att offentliggöra både realtids- och historisk data (var & när snöröjning genomförts). Konsekvensen av att informationen inte är riktig bedöms dock som **måttlig (1)** då det är troligt att endast enskilda individer eller kommunen själv erfar lindriga besvär.

### Vägledning avseende klassningsnivå – Tillgänglighet

I denna IoT-tillämpning är klassningsnivån inte särskilt hög för tillgängligheten, vare sig det rör sig om realtids- eller historisk data då den inte är avgörande för utförandet av grunduppgiften: snöröjning. Däremot kan den självklart skapa vissa lindriga besvär för både enskilda individer och kommunen samt andra organisationer varför den kan bedömas som **måttlig (1)**.

System med positionering av renhållningsfordon och avfallscontainrar

I den här IoT-tillämpningen används GPS-data främst för att positionsbestämma olika typer av avfallscontainrar och skicka denna information till ytterligare ett system för koordinering av utlåning och upphämtning av containrarna. Med hjälp av systemet kan man exempelvis inventera antal containrar inom ett avgränsat geografiskt område, bevaka att containrar inte förflyttas ut ur ett geografiskt område utan tillstånd samt identifiera exakta koordinater vid upphämtning.

### Vägledning avseende klassningsnivå – Konfidentialitet

Vid klassning av konfidentialiteten är det viktigt att beakta den aggregerade informationen och inte endast de specifika koordinaterna som IoT-sensorn skickar vidare. I systemet kombineras GPS-data i form av koordinater med kundinformation som namn, organisationsnummer, adresser samt fotografier av platser för återrapportering. Med hänsyn till att systemet innehåller person-uppgifter är en rimlig klassningsnivå **betydande (2)**.

### Vägledning avseende klassningsnivå – Riktighet

Informationen i allmänhet och GPS-data i synnerhet bör kunna klassas som **betydande (2)** med hänsyn till riktighet. Informationen behöver vara korrekt för att containrar ska kunna hämtas och hanteras på rätt sätt och felaktig information leder till dels merarbete och dels högre kostnader. Därutöver kan organisationens eller kommunens förtroende skadas och om avfallscontainrar innehåller miljöfarligt avfall finns risken att det inte tas om hand i tid.

### Vägledning avseende klassningsnivå – Tillgänglighet

Även om tillgängligheten till systemet i allmänhet och information om GPS-data och containrars koordinater i synnerhet inte är direkt avgörande för att organisationen ska kunna genomföra sin verksamhet så förlitar man sig på att

informationen är tillgänglig i hög grad. Skulle systemet och informationen vara otillgänglig i mer än 24h klassas tillgänglighetsaspekten som **betydande (2)**. Detta på grund av att effektiviteten märkbart går ner samt att kostnader ökar.

## Övervakning av bräddningsnivåer

Bräddningsnivåövervakning syftar till att mäta om bräddningsnivåer av dag- och avloppsvatten överstiger vissa nivåer och riskerar att rinna ut i ytvatten-täkter. Detta är av vikt för att kommunen ska kunna uppfylla ställda krav i bland annat miljöbalken och Naturvårdsverkets föreskrifter. Genom övervakningen hinner kommunen (eller utsedd ansvarig) vidta åtgärder innan eventuell bräddning sker samt prioritera det återkommande underhållsarbetet i en eller flera VA-anläggningar.

### Vägledning avseende klassningsnivå – Konfidentialitet

När information från denna typ av IoT-tillämpning ska klassas med hänsyn till konfidentialitet är det rimligt att anta att en viss typ av förtroendeskada kan uppstå. VA-verksamhet är ofta utkontrakterad på ett kommunalt bolag varför eventuell information om breddningar inte bara drabbar bolaget utan även kommunen. Det är sannolikt att klassningen når nivån **betydande (2)** med hänsyn till att förtroendeskadan kan skapa en kännbar påverkan i flera organisationer.

### Vägledning avseende klassningsnivå – Riktighet

När riktigheten ska bedömas för denna tillämpning bör man beakta att informationen ligger till grund för beslut och prioriteringar och att det därför krävs att man till stor del kan lita på den. En rimlig bedömning är att nivån är **betydande (2)** i detta fall. Om beslut och prioriteringar sker på felaktiga grunder kan det orsaka stora besvär för enskilda individer och miljö men också en kännbar ekonomisk påverkan då åtgärder ofta är kostsamma.

### Vägledning avseende klassningsnivå – Tillgänglighet

Informationen kan i denna IoT-tillämpning ha mycket högt ställda krav på tillgänglighet vid olika tillfällen. Breddningar kan pågå i 10-60 minuter och om akuta åtgärder behöver vidtas måste informationen vara tillgänglig så att rätt åtgärder vidtas i rätt tid. Konsekvensen vid avsaknad av mätvärden blir likt bedömningen av riktighet att enskilda individer och miljön kan utsättas för stora

besvär. Dessutom kommer underlag som behövs för rapportering till tillsyns-myndigheter att saknas. En rimlig bedömning blir då **betydande (2)**.

# Informationssäkerhet inom fastighetsområdet & IoT

Flertalet av de smarta produkter och tjänster som utvecklas och marknadsförs inom fastighetssektorn bygger på åtkomst till kontinuerligt insamlade dataströmmar. Det kan gälla data om byggnaders energi- och vattenflöden, luftkvalitet och konstruktiva tillstånd, men också data om de aktiviteter som genomförs i eller i nära anslutning till byggnaden.

I denna skrift kan du läsa om grunderna för hur man med utgångspunkt i ett systematiskt informationssäkerhetsarbete, kan utveckla en organisatorisk förmåga att möta efterfrågan på denna typ av dataströmmar.

Primär målgrupp för skriften är kommunernas säkerhetsorganisationer och fastighetsorganisationer. Sekundär målgrupp är övriga fastighetsägare, konsulter och leverantörer som verkar inom fastighetsbranschen.

Upplysningar om innehållet
Bo, Baudin, bo.baudin@skr.se


ISBN/Beställningsnummer: 978-91-8047-001-8
Text: Thomas Nilsson & Eilia Etminan, Certezza AB; Lars Lidén, Meta fastighetsadministration
Illustration/foto: Advant
Produktion: SKR

**ISBN** 978-91-8047-001-8
Beställ eller ladda ner på webbutik.skr.se
**Post:** 118 82 Stockholm | **Besök:** Hornsgatan 20
**Telefon:** 08-452 70 00 | www.skr.se

Sveriges Kommuner och Regioner