Underlag 3 – FKU

Stöd vid kravställning och förslag på mervärden vid FKU

Säkerhetsteknik 2020

Referensnummer 10511

2021 08 05

Innehållsförteckning

Bakgrund

I nedanstående lista finns en förteckning ställda kraven och de parametrar som kan preciseras, eller vid behov kompletteras med, i den förnyade konkurrensutsättningen. I underlaget finns exempel på hur krav kan följas upp.

För flera områden finns även bifogad dokumentation som innehåller ytterligare exempel på krav på leverantörer och för utveckling av t ex it-säkerhet för beställares verksamheter. En upphandlande myndighet kan välja om den vill formulera en precisering eller komplettering som ett obligatoriskt krav eller ett önskemål/mervärde i den förnyade konkurrens-utsättningen.

1. Informationssäkerhet

Ramavtalsleverantörens ansvar för medarbetare, och att Underleverantörens medarbetare följer riktlinjer för säkerhet och informationssäkerhet enligt nedan och ramavtal.

Informationssäkerhet

För att tjänsten ska anses säker och ge förväntad trygghet ska tekniken ge skydd för information. Det förutsätter att samtliga delar i den levererade larmkedjan fungerar och samverkar. Information som lagras och överförs i den tekniska lösning som leverantören tillhandahåller för en avtalad tjänst, ska vara skyddad avseende konfidentialitet, riktighet och tillgänglighet.

Tjänsten ska vara utformad så att oplanerade avbrott kan hanteras utan att information går förlorad. Känsliga uppgifter som överförs över öppet nät ska vara krypterade.

Molntjänster

För kravställning gällande nyttjande av molntjänster hänvisas till nedanstående länk.
https://skr.se/skr/naringslivarbetedigitalisering/digitalisering/arkitektursakerhet/molntjanster/vagledningarmolntjanster.29885.html"

Allmänna krav och krav på leverantör

Systematisk och strukturerat informationssäkerhetsarbete

Leverantören ska ha ett strukturerat och dokumenterat ledningssystem för informationssäkerhet. Ledningssystem för informationssäkerhet ska omfatta samtliga delar av leverantörens verksamhet som medverkar i fullgörandet av detta avtal och ingående leverans. Ledningssystem för informationssäkerhet ska vara aktivt under hela tiden avtalet och under tiden som leveransavtal är aktiva. Ledningssystem för informationssäkerhet (LIS) ska vara baserad på SS-EN ISO/IEC27001:2017.

Leverantör ska redovisa sitt ledningssystem för informationssäkerhet minst innehållande punkterna 1 - 5 nedan. Som alternativ till redovisning av ledningssystem för informationssäkerhet i sig godtas att
leverantör redovisar gällande certifikat avseende ett ledningssystem för informationssäkerhet som minst motsvarar punkterna 1 - 5 nedan. Certifikat med tillhörande Uttalande om Tillämplighet, UoT (Statement of Applicability, SoA) ska bifogas som svar.

Ledningssystem för informationssäkerhet ska minst innehålla punkterna 1 - 5 nedan:

1. **Policy och organisation**
   Leverantören ska ha en informationssäkerhetspolicy samt en etablerad organisation som aktivt arbetar med informations- och IT-säkerhetsfrågor.

2. **Process för upprättande och dokumentation av informationssäkerhetsmål**
   Fastställande och tillämpning av en process för upprättande och dokumentation av informationssäkerhetsmål för relevanta funktioner och nivåer. Informationssäkerhetsmålen ska vara mätbara (om det är praktiskt möjligt), beakta tillämpliga informationssäkerhetskrav och resultat från riskbedömning och riskbehandling, kommuniceras samt uppdateras efter behov.

3. **Process för bedömning och behandling av informationssäkerhetsrisker**
   Fastställande och tillämpning av en process för bedömning av informationssäkerhetsrisker som upprättar och underhåller kriterier för riskacceptans och kriterier för bedömningar av informationssäkerhetsrisker. Processen ska säkerställa att upprepade bedömningar av informationssäkerhetsrisker genererar konsistenta, korrekta och jämförbara resultat. Processen ska omfatta att informationssäkerhetsriskerna identifieras genom tillämpning av processen för bedömning av informationssäkerhetsrisker för att identifiera risker förknippade med förlust av konfidentialitet, riktighet och tillgänglighet inom omfattningen för ledningssystem för informationssäkerhet. Processen ska omfatta att informationssäkerhetsriskerna analyseras genom att bedöma de potentiella konsekvenser som skulle uppstå om riskerna som identifierats realiseras. Vidare ska den realistiska sannolikheten för förekomsten av de risker som identifierats bedömas och risknivåer fastställas. Informationssäkerhetsriskerna ska utvärderas och resultaten av riskanalyser jämföras med de fastställda riskkriterierna. De analyserade riskerna ska prioriteras för riskbehandling. Bedömningar av informationssäkerhetsrisker ska genomföras med planerade intervall eller när betydande förändringar föreslås eller uppstår, med hänsyn till de kriterier som fastställs.

   Fastställande och tillämpning av en process för behandling av informationssäkerhetsrisker för att välja ut lämpliga alternativ för behandling av informationssäkerhetsrisker, med hänsyn tagen till resultaten av riskbedömningen samt fastställande av alla säkerhetsåtgärder som är nödvändiga för att införa valda alternativ för behandling av informationssäkerhetsrisker. Processen ska omfatta verifikation av att inga nödvändiga säkerhetsåtgärder har utelämnats. Processen ska leda till skapandet av ett uttalande om tillämplighet som innehåller de nödvändiga säkerhetsåtgärderna och motivering för inkludering samt om de är införda eller inte. Processen ska omfatta formulerandet av en plan för behandling av informationssäkerhetsrisker.

4. **Process för lämpligheten, tillräckligheten och verkan av ledningssystem**
   Fastställande och tillämpning av en process för att lämpligheten, tillräckligheten och verkan av ledningssystem för informationssäkerhet ständigt ska förbättras. Processen ska innefatta fastställande av vilka resurser som behövs för att upprätta, införa, underhålla och ständigt förbättra ledningssystem för informationssäkerhet samt säkerställande av att resurserna tillhandahålls. 5. Genomförande av interna revisioner Genomförande av interna revisioner med planerade intervall för att få information om huruvida ledningssystem för informationssäkerhet överensstämmer med kraven på ledningssystem för informationssäkerhet samt att ledningssystem för informationssäkerhet har införts och underhållits på ett ändamålsenligt sätt.

5. **Kontinuitetsplan och skydd mot obehöriga**
   Ramavtalsleverantören ska ha en kontinuitetsplan för sin verksamhet och it-system. Kontinuitetsplanen ska testas regelbundet. Ramavtalsleverantören ska skydda Kunds information som hanteras och förvaras i Ramavtalsleverantörens lokaler från obehöriga samt ha rutiner för hur denna information skyddas från obehöriga.

Förslag på krav vid FKU : Efterlevnad. Beskriv hur ovan ställda krav uppfylls.

Process och rutin för säkerställande av säker leverans.
En process ska finnas som säkerställer att mjukvara och hårdvara som utvecklas och/eller anskaffas är säker med avseende på:

- Personalens kompetens och utbildningar inom säker systemutveckling
- Test och verifiering så som kodgranskningar, penetrationstester och härdning av system
- Monitorering och detekteringsförmåga, dvs möjligheten att upptäcka, respondera och avhjälpa sårbarheter som kan uppstå i systemet.
- Skydd av data så som kryptering, skydd mot avlyssning (kablage), säkerställa att personuppgifter hanteras enligt GDPR, säkerhetsskyddslagen följs.
- Incidenthantering och rapportering av incidenter ska ske enligt rekommendationer och regler satta av EU och/eller lokala myndigheter så som MSB.

Förslag på krav vid FKU: Efterlevnad: Beskriv hur ovan ställda säkerhetskrav uppfylls

Lagar och förordningar – Under avtalsperioden ska leverantör följa gällande lagar, förordningar, föreskrifter och relevanta standarder. Om det under avtalsperioden tillkommer nya lagar, förordningar, föreskrifter eller standarder inom aktuellt område så skal även dessa gälla och följas av leverantör.

Leverantören ska vidta de erforderliga tekniska och organisatoriska åtgärder som krävs för att skydda de personuppgifter som behandlas.

Säkerhetsskydd - I det fall bedömning görs att leveransen omfattas av säkerhetsskydd enligt säkerhetsskyddslagen, ska tillämpliga bestämmelser i nämnda lag beaktas. Säkerhetsskyddsavtal ska ingås, säkerhetsprövning och registerkontroll ska ske enligt rekommendationer med leverantör samt dess underleverantör.

Right to audit – detta ska finnas och kopplas till ovan punkter.

Avropsberättigad har rätt att genomföra uppföljning i syfte att kontrollera att leverantören följer de krav som framgår av kontraktet. Ytterligare rätt till uppföljning kan framgå av tecknat säkerhetsskyddsavtal. Vid uppföljning ska Avropsberättigad ha rätt att ta hjälp av en oberoende utomstående kontrollorganisation. Avisering om uppföljning ska normalt göras senast två veckor före uppföljningens genomförande

2. Krav på teknisk lösning

Samtlig information och aktivitet som sker i systemet ska skyddas utifrån konfidentialitet, riktighet och tillgänglighet. Nedan anges övergripande krav som leverantören ska beskriva sin efterlevnad mot.

Konfidentialitet
Information som lagras och överförs i den tekniska lösning som leverantören tillhandahåller för implementering av avtalad tjänst, ska vara skyddat mot obehörig åtkomst, med hänsyn till risken för röjande, ändring och förvanskning. Information som lagras i och överförs med en molntjänst ska vara krypterad. Krypteringsnycklar ska stå under kontroll av ägaren av informationen av data. Via behörighetskontroller ska larmoperatörer och administratörer ges specifika rättigheter för vad deras uppgift kräver.

Behörigheter ska årligen följas upp av leverantör. Administratörsrättigheter ska loggas och vara skyddade mot insyn och förändring. Den som kan administrera administratörsrättigheter ska inte kunna administrera loggar.

Riktighet
Information som lagras och överförs i den tekniska lösningen som leverantören tillhandahåller för implementeringen av en avtalad tjänst, ska vara skyddad mot obehörig ändring, med hänsyn till risken för röjande, ändring och förvanskning.

Tillgänglighet
Information som lagras och överförs i den tekniska lösning som anbudsgivaren tillhandahåller för implementeringen av en avtalad tjänst, ska hålla en hög nivå vad gäller tillgänglighet och kvalitet i hela den levererade larmkedjan. Tjänsten ska vara utformad så att oplanerade avbrott kan hanteras utan att information går förlorad*. Krav på tillgänglighet specificeras i detalj i SLA.*

Spårbarhet/Oavvislighet
Leverantören ska säkerställa att det finns loggar som registrerar händelseförlopp och åtgärder för samtliga larmanrop. Loggar ska utvisa om information har förändrats, vad som förändrades, vem som genomförde förändringen och tidpunkt för förändringen.

Det ska vara möjligt att identifiera vem som gjort vad genom hela larmkedjan, från initiering av larm till kvittens av larmmottagning alternativt utförare.

Förslag på krav vid FKU : Efterlevnad: Beskriv hur ovan ställda säkerhetskrav uppfylls.

3. Fastighetsnät och infrastruktur

Nr	Krav	Kommentar
a	Entreprenören eller antagen underentreprenör ska vara certifierad för installation av flerfunktionsnät (datanät), koppar och fiber och kunna lämna begärda garantier/certifikat. Entreprenören ansvarar för att de i beskrivningen föreskrivna anläggningarna installeras på	*Krav ställt i ramupphandling. Vid FKU bör kontroll göras för att säkerställa efterlevnad.*

	ett fackmannamässigt sätt, varför entreprenören är skyldig att anlita personal (arbetsledning och montörer) med minimum 5 års erfarenhet inom data- och teletekniska installationer. Montörer/representant för entreprenören ska ha genomgått utbildning i de krav som SS-EN 50173-1/-2/50174 ställer för klass-länk och kategorier enligt följande: • Kategori 5e Class D: upp till 100 MHz; • Kategori 6 Class E: upp till 250 MHz; • Kategori 6A Class EA: upp till 500 MHz; • Kategori 7 Class F: upp till 600 MHz; • Kategori 7A Class FA: upp till 1 000 MHz	
b	- ELSÄK-FS 2008:1-3 Elsäkerhetsverkets författningssamling, inklusive gällande ändringar i ELSÄK-FS. - SS 436 40 00 Elinstallationsreglerna senaste utgåvan. - SS 437 01 02 Elinstallationer för lågspänning – Vägledning för anslutning, mätning, placering och montage av el- och teleinstallationer. - SS EN 50 173-1, Fastighetsnät för informationsöverföring – Generella kabelnät - Del 1: Allmänna fordringar. - SS EN 50 173-x, Fastighetsnät för informationsöverföring – Generella kabelnät. - SS EN 50 174-1, Fastighetsnät för informationsöverföring – installation av kablage – Del 1: Planering och kvalitetssäkring. - SS EN 50 174-2 & 3, Fastighetsnät för informationsöverföring – Installation av kablage – Del 2 och 3: Planering och genomförande av installation inomhus och utomhus. - Robust Fiber, Anvisningar för Robusta Fastighetsnät – Huvuddokument.* - Robust Fiber, Bilaga 1 Förläggning av fiberoptiska Fastighetsnät.*	*Krav ställt i ramupphandling. Vid FKU bör kontroll göras för att säkerställa efterlevnad.*

	* Hänvisning avser Svenska Stadsnätsföreningens rekommendationer för Robusta Fastighetsnät och utgör ett komplement till Robust Fiber för att därmed säkerställa kommunikation ända fram till överlämningspunkten i slutkundens bostad/lokal inne i fastigheten. Dessa dokument finns förnärvarande på Svenska stadsnäts hemsida via länk från Robustfibers hemsida ”Robust digital infrastruktur”	

Förslag på krav vid FKU : Efterlevnad: Beskriv hur ovan ställda säkerhetskrav uppfylls.

Kravmatris

Nr	Krav	Kommentar
Allmän	Leverantören ska beskriva sitt Ledningssystem för Informationssäkerhet (LIS). Om ledningssystemet är certifierat enligt SS-EN ISO/IEC 27001 ska certifikat bifogas anbudet.	
Allmän	Säkerhetsskyddsavtal ska tecknas ifall det bedöms relevant. Leverantören ska följa de ingående detaljerna baserat på SUA klassning.	
Allmän	Leverantören ska säkerställa att adekvata bakgrundskontroller genomförs av sin personal innan arbete genomförs. Vid SUA ska RK (riskkontroll) genomföras enligt nivå beskriven i kontrakt.	Precisera krav i kontrakt
Audit	Test och verifiering så som kodgranskningar, penetrationstester och härdning av system ska genomföras regelbundet, eller vid behov, av leverantören. Detta gäller de relevanta ingående komponenterna/systemen i aktuell leverans.	
Audit	Beställaren har rätten att genomföra granskningar för att säkerställa kraven i avtalet. (”right to audit”)	
Audit	Beställaren ska ha åtkomst till resultatet av leverantörens egenkontroller eller externa granskningar initierade av leverantören själv. (Interna/externa revisioner och/eller penetrationstester)	
Audit	Leverantören ska stödja beställaren vid granskningar där en tillsynsmyndighet initierar granskningen av informationshanteringen	
Behörighet	Behörigheter – kontroll ska ske av alla It-konton. Ej aktiva konton ska inaktiveras.	
Behörighet	Behörigheter – Tilldelning av behörigheter ska vara strikt och uppstyrd av beställare. Least privilege samt Need-to-know principer ska tillämpas.	

Behörighet	Behörigheter – användaridentiteter ska kunna skapas automatiskt och integration med exempelvis kataloger (AD) bör vara möjligt. Indelning i grupper ska vara möjligt för att separerar resurserna och behörigheter.	
Behörighet	Flerfaktorsautentisering ska tillämpas på alla publikt exponerade tjänster. Där flerfaktorsautentisering inte stöds ska unika och komplexa lösenord nyttjas.	
Behörighet	Separata konton för systemadministrativa behörigheter.	
Behörighet	Skydd mot obehörig åtkomst ska finnas, både extern (via internet) åtkomst såväl som intern (lokala nätverk) obehörig åtkomst.	
Behörighet	Reparation och service av utrustning ska ske på ett sådant sätt att obehöriga (servicetekniker etc) inte får tillgång till material. Om detta inte är tekniskt möjligt ska mitigerande åtgärder finnas på plats, så som tecknande av avtal etc..	
Crypt	Alt 1 : Data ska skyddas med kryptering vid lagring samt vid överföring och kommunikation./ Alt 2: All data som bedöms känslig ska krypteras i lagrat tillstånd samt vid överföring.	Välj alternativ 1 eller 2.
Crypt	All kryptering, sessionsetablering och nyckelutbyte ska ske med publika, välgranskade och säkra algoritmer och protokoll.	
Crypt	Inga defaultnycklar eller nycklar som delas med andra kunder ska användas. Alt 1 : Kryptering ska genomföras med allmänt erkänd krypteringsmetod med tillräcklig nyckellängd. Alt 2: Alternativ: ”Kryptering ska genomföras med allmänt erkänd krypteringsmetod med tillräcklig nyckellängd enligt gällande ***”vägledning för grundläggande kryptering***” som publiceras av MSB”	Välj alternativ 1 eller 2.
Data	All data i systemet, så som inspelat material, ska skyddas mot förstöring, förändring och förvanskning.	
Data	Leverantören ska säkerställa att tillfredsställande säkerhet finns vid eventuellt överförande av inspelat material.	
Infra	Härdning av system ska genomföras - Säkerställ att funktioner som inte behövs för önskvärd funktionalitet i informationssystemen stängs av, blockeras eller avinstalleras.	
Infra	Endast tillåten utrustning får kopplas till nätverket.	
Infra	Systemet ska kunna installeras och separeras från övrig IT-miljö för att skapa kontrollerade trafikflöden mellan segmenten om önskvärt.	
Infra	Endast tillåten mjukvara får köras i it-miljön (Vitlistning).	

Infra	Filtreringsfunktioner ska finnas som skyddar mot att oönskad trafik kan flöda fritt i nätverket.	
Mon	Loggar ska kunna exporteras till SIEM lösning. Loggar ska skyddas mot obehörig åtkomst och/eller förvanskning.	
Mon	Övervakning ska vara möjlig av händelser i it-miljön med manuella, tekniska och automatiska åtgärder.	
Mon	Loggning ska finnas och vara konfigurerbart. Samtliga säkerhetsrelaterade händelser ska loggas så som inloggningar, access och/eller förändring av data, systemhändelser etc	
OpSec	Säkerhetskopior ska skapas på information utifrån verksamhetens behov. Hantering av säkerhetskopior ska ske på ett säkert sätt. Test ska ske periodiskt för att det säkerställa att det går att återställa informationen utifrån tagna säkerhetskopior.	
OpSec	Säkerhetsuppdateringar ska ske snarast och senast inom 3 dagar efter att de publicerats. I de fall uppdatering ej är möjlig ska tillfredställande mitigerande åtgärd införas.	
OpSec	Hantering av säker destruering av hårdvara ska finnas.	
OpSec	Reparation och service av övervakningsutrustning ska ske på ett sådant sätt att obehöriga inte får tillgång till materialet. Om inte detta kan ske ska avtal gällande säkerhet tecknas med serviceföretaget.	
OpSec	Säker radering och gallring av data ska vara möjligt i systemet. Automatiserad funktion ska finnas för exempelvis säker radering av inspelat material efter satt bevarandetid. Återskapande av data ska ej vara möjligt.	
Övrigt	*Ställ krav på hur information i systemet får användas, lagras samt när och hur uppgifter ska raderas.*	*Görs i PUB-avtal och i allmän kravställning*

Följ upp efterlevnad: Beskriv hur ovan ställda säkerhetskrav uppfylls.

4. Mekaniska och elektromagnetiska låsenheter

Generellt ska senaste utgåvan av regelverk gälla om inget annat anges.

Bra att ha med:
Service utav lås bör ske enligt tillverkarens anvisningar och intervall. Min 1 ggr år. Kan med fördel innefatta dörrstängare, dörrautomatik, skjutdörrsautomatik och liknande.

Nr	Krav	Kommentar
a	Leverantör ska vara godkänd anläggarfirma Låsanläggningar SSF1040. Alternativt medlem i SLR Sveriges Lås och Säkerhetsleverantörers Riksförbund. Auktoriserat Låsföretag	*För att inte utesluta bra låssmeder på framförallt mindre orter är SLR ett alternativ.* *https://slr.se/fretag/om-slr/*
b	Lås ska uppfylla SSF 3522. Låsklass anpassas till respektive objekt. Not: Klass 3 är grundkravet i samtliga skyddsklasser.	*Kravet finns även under digitala nycklar lås då med krav på minst klass 3. Klass 2a kan vara aktuellt pga utrymning.*
c	Utrymning och frångänglighetskrav ska alltid beaktad vid låsinstallationer, förändringar och utbyten av låsinstallationer.	
d	Ta vid FKU med de vanligaste låskomponenterna för att få A-pris. A-pris ska gälla under hela avtalstiden om de indexregleras.	*Resor, arbetsledning dokumentation m.m. kan ingå i A-pris.*
e	Innefattas låscylindrar av upphandlingen ställs krav på den önskade nivån som leverantören ska kunna leverera. - Registrerade (spärrade) låssystem - Patenterade (juridiskt skyddade) nycklar och nyckelämnen	

5. Inbrottslarmsystem

Generellt ska senaste utgåvan av regelverk gälla om inget annat anges.

Nr	Krav	Kommentar
a	Följande typer av larm ska finnas i offererat inbrottslarm : till och frånkopplingskontroll Larm överförs i format där sektion och sektionstext framgår, tex. SIA-format. Larmöverföring ska utföras enl. SSF 130 i avsedd larmklass.	
b	Ange exempel funktionskrav	Kontroll görs mot egen larmcentral/certifierad så att uppgifter kan över föras och hanteras
c	Leverantör ska ha polistillstånd för larminstallation och vara certifierade som larminstallatör enligt SSF 1015, lägst larmklass 1.	
d	Alla installationer ska utföras enligt SSF 130 i kravställd larmklass.	

e	Anläggarintyg ska alltid utfärdas vid övertagande, ombyggnation eller nyinstallation enligt SSF 130. Utförs enligt SSF 1058 Anläggarintyg inbrottslarm.	
f	Arbetsledning eller tillgänglig annan av L´s personal ska inneha certifikat som behöriga ingenjörer för inbrottslarm enligt SFF 1016 regelverk.	*Avser personal*
g	Material ska vara godkänt enligt SSF1014	*Underförstått i och med kravet på SSF 130, men vanligt att det förtydligas.*
h	Utdrag ur polisens belastningsregister utförs enligt kraven i SSF130. Dokumentation redovisas för beställaren vid begäran.	
i	Infällda magnetkontakter i fönster och dörrar ska ej vara av förspänt utförande.	*Larmklass 3 eller högre kan utanpåliggande förspända magnetkontakter installeras.*
j	Larm från övertäckningsskydd sk. Antimask ska utföras med egen sektion som går att särskilja i systemet.	*Detta för att larmcentralen ska veta om det är övertäckningsskydd som larmar. Sk. Trippelbalansering är ok.*
k	Alla i systemet ingående komponenter ska vara sabotageskyddade och avge larm i systemet.	
l	Hantering av dokumentation och personuppgifter se. SSF 130 respektive GDPR.	
m	System vid nyinstallation bör vara icke proprietärt. Systemet bör vara en produkt som finns tillgänglig hos grossist för flera oberoende installatörer på den svenska marknaden. En produkt anses inte leverantörsoberoende om tillgänglighet eller pris samt programmering eller driftsättning styrs av annan konkurrerande leverantör vid inköp, service eller installation. Programmering och driftsättning av en leverantörsoberoende produkt ska kunna utföras fullt ut av oberoende leverantörer.	Krav kan ställas på att systemet inte ska vara proprietärt.
n	Inbrottslarmet kan helt vara integrerat i passerkontrollsystemet.	*Kan många gånger bli kostnadseffektivare. Samma kablage, samma centralutrustning.* *Ange krav på backupptid om den ska avvika från SSF 130 i angiven larmklass, gällande passerkontrolldelen eller förtydliga att det är samma.*

6. Överfallslarm (personlarm)

(Överfallslarm)

Hanteras i AMA under inbrottslarm

Nr	Krav	Kommentar
a	Ange funktionskrav. Se exempel på krav nedan.	*Ange om krav finns på koppling till certifierad larmcentral, larmcentral och/ eller tjänsteleverantör.*
b	Knappar för överfallslarm ska vara av utförande dubbeltryck. Ska vara av modell som inte kräver spänningsmatning.	*Mindre falsklarm.*
c	Knappar för överfallslarm ska vara av modell som inte kräver spänningsmatning.	*Blir problem vid strömavbrott/spänningsbortfall.*
d	Funktion ”bråklarm” kan användas om verksamheten medger detta.	*Larmet går inte till vaktbolaget utan hanteras internt på plats. Kan ofta vara lättare att använda än överfallslarm vid lite ”mindre hotfulla situationer”.*
e	Fasta överfallsknappar ska märkas med klartext ”ÖVERFALLSLARM” (alt. ”BRÅKLARM”)	
f	Indikering för utlöst överfallslarm utförs och placeras i samråd med beställaren med beaktande av risk med att indikeringen kan förvärra situationen.	
g	Bärbart överfallslarm inom objekt kan utföras med eller utan positionering beroende på objekt, storlek ,risk och krav.	*Positionering är kostnadsdrivande.*
h	Överfallslarm för verksamheter som är ambulerande ska vara av modell som går på mobila nätet med minst funktioner för överfallslarm, kvittens mottaget larm, medhörning och positionering.	*Det finns tilläggsfunktioner och tjänster kopplade till bärbara överfallslarm med positionering. Kravställs efter behov.*
i	Funktion för larmutskick inom verksamheten via tex. SMS, personsökare rekommenderas. Kravställs vid behov.	

7. Kameraövervakning

Länk till lag gällande kameraövervakning

https://www.imy.se/verksamhet/kamerabevakning/kamerabevakningslagen/

Myndigheter och bland annat aktörer inom privat hälso- och sjukvård och privat skolverksamhet behöver ansöka om tillstånd om de vill kamerabevaka en plats dit allmänheten har tillträde.

https://www.imy.se/verksamhet/kamerabevakning/offentlig-verksamhet/

Tidigare utfärdade tillstånd gäller fortfarande.

Kameratillstånd som är som är utfärdat innan 25 maj 2018 gäller fortfarande för myndigheter och andra som utför en uppgift av allmänt intresse

Generellt ska senaste utgåvan av regelverk gälla om inget annat anges.

Bildöverföringssystem - tv-övervakningssystem är den korrekta AMA benämningen.

Nr	Krav	Kommentar
a	Reparation och service av övervakningsutrustning ska ske på ett sådant sätt att obehöriga inte får tillgång till materialet. Om inte detta kan ske ska avtal gällande säkerhet tecknas med serviceföretaget.	*Övergripande krav finns även under avsnittet Informationssäkerhet*
b	Leverantören ska var behjälpliga med framtagande av underlag för tillståndsansökan för kameraövervakning.	*Kan upphandlas så att det ingår under dokumentationen av CCTV anläggningar.*
c	Leverantören ska vara behjälpliga med framtagande av upplysningsskyltar och montage av dessa.	
d	Utförande enligt SSF 1060.	*Ge mervärde eller ställer krav på SSF 1060.*
e	Godkänd anläggarfirma enl. SSF 1061	*Ge mervärde eller ställ krav på SSF 1061.*
f	Systemintyg ska/bör alltid utfärdas vid övertagande, ombyggnation eller nyinstallation enligt SSF 1060. Utförs enligt SSF 1081 Systemintyg för kameraanläggning	*Bör-krav i ramavtal. Kan ställas som krav.*
g	Glöm inte 11-14§§ MBL om arbetsgivares förhandlingsskyldighet med facket gällande kameraövervakning på arbetsplats.	
h	System vid nyinstallation bör vara icke proprietärt. Systemeten bör vara en produkt som finns tillgänglig hos grossist för flera oberoende installatörer på den svenska marknaden. En produkt anses inte leverantörsoberoende om tillgänglighet eller pris samt programmering eller driftsättning styrs av annan konkurrerande leverantör vid inköp, service eller installation. Programmering och driftsättning av en leverantörsoberoende produkt ska kunna utföras fullt ut av oberoende leverantörer.	*Krav kan ställas på att det ska vara icke proprietärt.*

8. Brandskyddssystem

Rapport gällande onödiga larm

https://rib.msb.se/filer/pdf/17729.pdf

Branddetekterings- och brandlarmsystem är den korrekta AMA benämningen för brandlarm.

Det är AFS 2009:2 ställer krav på Utrymningslarmssystem.

Nr	Krav	Kommentar
a	Krav på funktioner.	*Ange vilka larm som ske kunna överföras till certifierad larmcentral, larmcentral och/eller tjänsteleverantör.*
b	Allt brand och utrymningslarm ska följa SBF 110 inkl. normativa bilagorna.	*Kontrollera*
c	Orienteringsritningar enligt SBF1021	*Dock underförstått då SBF 110 åberopas men kan vara bra att förtydliga.*
d	*För anläggning med TUL (talat utryckningslarm) kan krav ställas på att anläggningen ska uppfylla SBF 502.*	*När så BBR kravet ställs eller egen ambition.*
e	*FTR 110*	*Svensk försäkring. Försäkringsförbundet tekniska rekommendation.* Mer info finns på följande länk. https://www.svenskforsakring.se/globalassets/forsakringstekniska-rekommendationer/ftr-110-2-brandlarm.pdf
f	AFS 2009:2, Arbetsplatsens utformning	*Avser utrymning*
g	AFS 2008:13, Signaler och skyltar	
h	LSO (SFS2003:778)	*Lagen om skydd mot olyckor*
i	Brandskydd i boverkets byggregler kap 5	
j	Arbetsledning eller tillgänglig annan av L´s personal ska inneha certifikat som behöriga ingenjörer för brandlarm enligt SBF 1007 regelverk.	*Kontrolleras*
k	Tider för larmdonsprov specificeras tex. vardagar 07:00-08:00.	*Förenklar för verksamheterna.*
l	Tillsyn och skötsel av brand och utrymningslarm enligt SBF 110.	
m	Samplande system bör/kan övervägas där det av bla arbetsmiljöskäl är befogat.	*Ex. ljusgårdar, hisschakt där arbetsmiljön för provning av detektorer blir resurskrävande.*
n	Material ska vara enligt SS-EN 54.	
o	Brandlarm ska leveransbesiktigas enl. SBF 110	

p	Brandlarm ska revisionsbesiktigas 1ggr/år enligt SBF 110	
q	Anläggningsskötare rekommenderas vara utbildad enligt SSF 110 bilaga D.	
r	Månadsprov utförs av anläggningsskötare, kan med fördel utföras av verksamheten om denna är anläggningsskötare.	*Beror på verksamhetens utformning och kompetens.*
s	Så kallade kombilarm (inbrottslarm med brandvarning) bör kontrolleras och underhållas i enlighet med SBF 110.	*Nivån anpassas till respektive anläggning/avtal/upphandling.*
t	System vid nyinstallation bör vara icke proprietärt. Systemeten bör vara en produkt som finns tillgänglig hos grossist för flera oberoende installatörer på den svenska marknaden. En produkt anses inte leverantörsoberoende om tillgänglighet eller pris samt programmering eller driftsättning styrs av annan konkurrerande leverantör vid inköp, service eller installation. Programmering och driftsättning av en leverantörsoberoende produkt ska kunna utföras fullt ut av oberoende leverantörer.	*Krav kan ställas på att systemet ska vara icke proprietärt.*

9. Passagesystem

(Entré- och passerkontrollsystem är den korrekta AMA benämningen)

Nr	Krav	Kommentar
a	Tillgänglighet och frångänglighet beaktas vid installationer, förändringar och utbyten av passerkontrollsystem	*Ställ krav på utformning av kodtastatur, höjer på kortläsare tryckknappar m.m.*
b	System vid nyinstallation bör vara icke proprietärt. Systemeten bör vara en produkt som finns tillgänglig hos grossist för flera oberoende installatörer på den svenska marknaden. En produkt anses inte leverantörsoberoende om tillgänglighet eller pris samt programmering eller driftsättning styrs av annan konkurrerande leverantör vid inköp, service eller installation. Programmering och driftsättning av en leverantörsoberoende produkt ska kunna utföras fullt ut av oberoende leverantörer.	*Krav kan ställas på att det ska vara icke propretärt.*
c	*Passage system kan helt vara integrerat i inbrottslarmsystemet.*	*Kan många gånger bli kostnadseffektivare. Samma*

		kablage, samma centralutrustning. *Ange krav på backupptid om den ska avvika från SSF 130 i angiven larmklass, gällande passerkontrolldelen eller förtydliga att det är samma.*
d	Systemen ska vara kompatibelt med GDPR	

10. Digitala nycklar

Information om kravställning för digitala nycklar.

https://www.fastighetsagarna.se/fakta/fakta-for-fastighetsagare/forvaltning/digitala-losningar/digitala-lassystem/

”övrig vägledning för nyttjande av molntjänster gäller även i denna upphandling och bör beaktas - https://skr.se/skr/naringslivarbetedigitalisering/digitalisering/arkitektursakerhet/molntjanster/vagledningarmolntjanster.29885.html”

Nr	Krav	Kommentar
a	Lås eller låssystem bör inte vara uppkopplade publikt mot internet. Uppkoppling ska ske mot ett tekniskt nät eller ett nät där säkerhet kan garanteras.	
b	För batteridrivna lås gäller att batteritiden ska vara minst 3 år.	
c	Byte av batteri ska ingå i uppdraget	
d	Låssystem ska minst uppfylla krav enligt krav enligt SSF 3522 klass 3. Krav kan anges på klass 4 -7.	*Kontroll behöver göras över vad som erbjuds på marknaden innan krav ställs. Kan behöva samordnas med krav gällande avsnitt 2, Mekaniska och elektromagnetiska låsenheter.*
e	System vid nyinstallation bör vara icke proprietärt. Systemeten bör vara en produkt som finns tillgänglig hos grossist för flera oberoende installatörer på den svenska marknaden. En produkt anses inte leverantörsoberoende om tillgänglighet eller pris samt programmering eller driftsättning styrs av annan konkurrerande leverantör vid inköp, service eller installation. Programmering och driftsättning av en leverantörsoberoende produkt ska kunna utföras fullt ut av oberoende leverantörer.	*Krav kan ställas på att systemet inte ska vara proprietärt.*

11. Hållbarhet

Nr	Krav	Kommentar
	Avfallshantering och redovisning inom avtalet	*Redovisas vid årlig driftrapport?*
	Krav på miljövarubedömning av produkter	

12. Service

Vid övertagande av anläggningar med ny leverantör kan vid behov status-kontroller användas för att få en överblick av beståndet. Detta anges i FKU och prissätt av leverantör för avrop.

Nr	Krav	Kommentar
	Revisioner, rekommendation 1 gång per år.	*Inom avtal för säkerhetssystem benämns revisioner som tillsyner. Rekommendationen är att dessa sker 1 gång per år.*
	Reglering av avtalssumma där beståndet förändras kraftigt kan komponentpris upphandlas och regleras årsvis.	*Förslag är att ställa en +/- 5% spärr för minsta reglering av avtalssumman.*

13. Övrig

Nr	Krav	Kommentar
	Teletekniska installationer ska dokumenteras enligt SS 455 12 01.	*Är befintlig dokumentation utförd i tidigare utgåva kan denna krav ställas.*