Innehållstyp
Riktlinje

Dokumentnummer
1530039

Version
1.0

Godkänd av
Nilsson Monica

Godkänt datum
2020-08-18

Säkerhetsklass
0

Allmänna och säkerhetsklassade handlingar

Utdrag ur riktlinje Allmänna och säkerhetsklassade handlingar (v 2.0 godkänd 2020-08-18) för information till leverantörer och andra externa intressenter

1 Inledning

MittSverige Vatten & Avfall (MSVA) är ett kommunalt bolag och ska därför tillämpa offentlighetsprincipen. Offentlighetsprincipen ger allmänhet och massmedia rätt till insyn i det allmännas verksamhet, vilket bland annat omfattar rätten att ta del av allmänna handlingar. Det finns dock vissa begränsningar i rätten att ta del av allmänna handlingar.[1]

Med stöd av offentlighets- och sekretesslagen (OSL) kan vissa typer av uppgifter beläggas med sekretess, vilket innebär att uppgifterna omfattas av tystnadsplikt. Tystnadsplikten innebär ett förbud mot att röja uppgiften till obehöriga oavsett om det sker muntligen, genom att en handling lämnas ut eller på annat sätt.

En formell sekretessbedömning genomförs normalt sett först när en handling begärs ut. För att vi ska kunna hantera information på rätt sätt fram till dess ska all information värderas och klassificeras.

3 Säkerhetsklassificering av information

Vid en fullständig informationsklassificering bedöms aspekterna konfidentialitet, riktighet och tillgänglighet. Här behandlas enbart konfidentialitet eftersom det är den aspekt som har en direkt koppling till sekretess enligt OSL.

För att avgöra informationens säkerhetsklass använder MSVA en intern klassificeringsmodell med fem klasser. Säkerhetsklassning ska genomföras för all information, exempelvis i samband med att ett dokument upprättas och när innehållet ändas på ett sätt som kan påverka klassningen. Alla internt upprättade handlingar ska märkas med aktuell säkerhetsklass i sidhuvudet eller på annan lämplig plats (0, 1, 2, 3 eller 4).

Den interna säkerhetsklassningen anger vilket skydd informationen kräver och hur informationen ska hanteras.

3.1 Bedömning av säkerhetsklass

Utgångspunkten för klassificering av information är en bedömning av skadan (konsekvensen) som kan inträffa om informationen sprids till obehöriga, ändras felaktigt och/eller inte är tillgänglig. När det gäller konfidentialitet ska man därför bedöma konsekvenserna av att obehöriga tar del av information. För att undvika att stora mängder information klassificeras för högt ska orimliga konsekvenser inte beaktas. Av samma skäl ska bedömningen av enskilda uppgifter inte heller omfatta vad som kan hända om annan information röjs vid samma tillfälle.

I vissa fall kan en konsekvens uppstå enbart på grund av att uppgifter kommer ut oavsett om det finns någon intention att orsaka skada eller inte. Det kan till exempel röra känsliga personuppgifter eller uppgifter kopplat till anbud i samband med en upphandling.

[1] 2 kap §§ 1-2 Tryckfrihetsförordningen (TF)

I andra fall krävs det också att den som fått ta del av informationen använder den för att orsaka skada, begå brott och/eller genomföra förberedelser för sabotage, terrorism eller krig. Det kan exempelvis röra sig om kartmaterial, risk- och sårbarhetsanalyser, beskrivningar av skalskydd och driftinstruktioner. I dessa fall är det viktigt att analysera vad uppgifterna skulle kunna användas till av någon som har kunskap, förmåga och intention att orsaka skada för att kunna bedöma konsekvenserna

3.1.1 Säkerhetsklass 0

Avser allmän och öppen information. Informationen omfattas inte av sekretess och innehåller inga personuppgifter. Ingen negativ påverkan eller enbart en försumbar skada kan uppstå om informationen sprids.

3.1.2 Säkerhetsklass 1

Avser uppgifter av intern karaktär och allmänna handlingar som i vissa fall skulle kunna omfattas av sekretess, till exempel om uppgifterna sammanställs.

Att obehöriga tar del av informationen kan orsaka måttlig negativ påverkan på egen eller annan organisation och dess tillgångar, eller på enskild individ.

3.1.3 Säkerhetsklass 2

Avser uppgifter av intern karaktär och av allmänna handlingar som kan omfattas av sekretess enligt OSL.

Att obehöriga tar del av informationen innebär en betydande negativ påverkan på egen eller annan organisation och dess tillgångar, eller på enskild individ. Den drabbade verksamheten kan fullfölja sina uppdrag men det finns en risk för kännbar påverkan.

3.1.4 Säkerhetsklass 3

Avser uppgifter som omfattas av sekretess enligt OSL och som antingen ger en helhetsbild eller ger detaljerad information kopplat till särskilt skyddsvärda anläggningar/verksamhet som till exempel civila skyddsobjekt.

Att informationen sprids till obehöriga innebär en allvarlig negativ påverkan på egen eller annan organisation och dess tillgångar, eller på enskild individ. Det skapar stora svårigheter för den drabbade organisationen och verksamheten kan inte fullfölja sina uppdrag.

3.1.5 Säkerhetsklass 4

Avser uppgifter som omfattas av sekretess och som rör Sveriges säkerhet, så kallade säkerhetskyddsklassificerade uppgifter enligt säkerhetsskyddslagen. Typen av uppgifter som blir placerade i säkerhetsklass 4 är till stor del samma som för säkerhetsklass 3. För att handlingar ska bli inplacerade i säkerhetsklass 4 krävs det att uppgifterna rör säkerhetskänslig verksamhet. Det kan till exempel handla om totalförsvarsplanering oavsett verksamhetsområde, viktiga

dricksvattenanläggningar eller processnätet. Utöver att uppgifterna ska röra säkerhetskänslig verksamhet ska också konsekvensen av att uppgiften röjs påverka Sveriges säkerhet. Det räcker dock med att skadan för Sveriges säkerhet bedöms som ringa för att säkerhetsklass 4 ska bli aktuell.

Informationen ska märkas med säkerhetsklass 4 och klassificeras i enlighet med säkerhetsskyddslagen (2018:585) 2 kap. 5 §. Märkning ska ske enligt OSL och med aktuell säkerhetsskyddsklass med utgångspunkt från den skada som ett röjande av uppgiften kan medföra för Sveriges säkerhet. Indelningen görs enligt följande:

- *kvalificerat hemlig* vid en synnerligen allvarlig skada,
- *hemlig* vid en allvarlig skada,
- *konfidentiell* vid en inte obetydlig skada, eller
- *begränsat hemlig* vid endast ringa skada.

4 Hanteringsregler

Hanteringsreglerna gäller för handlingar eller uppgifter i respektive säkerhetsklass oavsett om det handlar om original eller kopior. Vid behov av avsteg från hanteringsreglerna för säkerhetsklass 1-3 ska beslut fattas av ansvarig chef på MSVA i samråd med säkerhetssamordnare. Inga undantag ges för säkerhetsklass 4.

När det gäller säkerhetsklass 0 finns det inga särskilda hanteringsregler eller begränsningar i hur informationen får spridas eller användas. Interna dokument ska dock märkas för att visa på att säkerhetsklassning har genomförts.

4.1 Generella hanteringsregler för säkerhetsklass 1-3

Alla medarbetare på MSVA har som inloggad tillgång till någon form av skyddsvärd information genom sina personliga behörigheter. För att säkerställa att obehöriga inte tar del av uppgifter ska arbetsdatorn låsas när den lämnas utan uppsikt inom MSVA:s lokaler. Utanför MSVA:s lokaler ska datorn förvaras under uppsikt eller låsas in. Motsvarande krav gäller för externa aktörer som har information från MSVA på sin arbetsdator.

Extern spridning av skyddsvärd information ska begränsas. Det finns dock tillfällen då det är nödvändigt att dela information, till exempel för att det är en förutsättning för att ett företag ska kunna utföra ett uppdrag/leverera en tjänst som vi har beställt eller för att en myndighet ska kunna utföra sin uppgift. Vid delning av skyddsvärd information ska åtgärder vidtas för att säkerställa att uppgifterna skyddas och hanteras på ett korrekt sätt. Se kapitel 7 Delning av information till externa aktörer för mer information.

Tänk på att en samling av handlingar, digitalt eller fysiskt, sammantaget kan få en högre säkerhetsklass än vad varje enskilt dokument har. En pärm med flera dokument i säkerhetsklass 2 kan exempelvis ge en helhetsbild som motsvarar säkerhetsklass 3.

Inbrott i lokaler/utrymmen där skyddsvärd information förvaras, förlust av dator/iPad/telefon eller andra misstankar om att obehöriga kan ha tagit del av skyddsvärd information ska anmälas till säkerhetssamordnaren. Kom ihåg att brott som begås mot MSVA alltid ska polisanmälas.

4.2 Säkerhetsklass 1

Det finns inga krav på begränsning av intern spridning av informationen inom MSVA. Uppgifterna ska dock behandlas och förvaras så att de skyddas mot obehöriga. Dokument ska till exempel inte ligga framme utan uppsikt i utrymmen där externa besökare har tillträde. Det bör också alltid genomföras en bedömning av vilka medarbetare som har behov av att ta del av uppgifterna och om behörighetsstyrning är lämplig, särskilt för personuppgifter.

Extern spridning bör begränsas och ska föregås av en sekretessbedömning. Om uppgifterna inte bedöms omfattas av sekretess kan de delas/lämnas ut och handlingar kan skickas med vanligt brev och öppen e-post.

Enskilda handlingar i säkerhetsklass 1 ska inte omfattas av sekretess. Om information från flera handlingar i säkerhetsklass 1 sammanställs kan i vissa fall den sammantagna informationen bli föremål för sekretess.

4.3 Säkerhetsklass 2

Spridningen av informationen ska vara begränsad och enbart ske till personer som:

- bedöms pålitliga ur säkerhetssynpunkt
- har tillräckliga kunskaper om hanteringen av skyddsvärd information
- behöver uppgifterna för sitt arbete

Fysiska handlingar ska hållas under god uppsikt eller förvaras i ett låst utrymme. Elektronisk förvaring ska ske så att endast behörig personal kan ta del av informationen, exempelvis genom behörighetsstyrning. Informationen får inte lagras i datamedier utanför organisationens brandvägg/externt, till exempel på en privat dator eller i en molntjänst. Förvaring av information i bil eller andra fordon utan uppsikt ska undvikas.

För utskrift ska skrivare med behörighetsskyddad utskrift eller lokal skrivare inom synhåll från den som skriver ut dokumentet användas.

Information får inte delas utan kryptering via e-post eller andra icke-godkända fildelningsverktyg. För mer information om kryptering se bilaga 8 Skapa krypterade filer. Verktyget ”Skicka stora filer” med krav på inloggning med e-legitimation/mobilt bankID för att kunna ladda ner filerna får användas. Verktyget finns på https://filer.sundsvall.se För mer information se Lathund – Hantera och skicka stora filer. Verktyget kan användas oavsett vem som är mottagare av informationen. Det är dock bara verksamheter och bolag inom Sundsvalls kommunkoncern som kan använda verktyget för att dela information.

För delning av information inom kommunkoncernen kan också information delas via det lokala nätverket genom att en mapp med begränsad behörighet upprättas på N: (gemensam). Om informationen skickas via brev ska rekommenderat brev användas.

Möten, samtal eller telefonsamtal där uppgifter i säkerhetsklass 2 diskuteras bör ske avskilt för att minska risken för att obehöriga tar del av informationen.

Dokument ska förstöras med dokumentförstörare eller lämnas i ett låst kärl för destruktion.

4.4 Säkerhetsklass 3

Spridningen av informationen ska vara mycket starkt begränsad och enbart ske till personer som:

- bedöms pålitliga ur säkerhetssynpunkt
- har tillräckliga kunskaper om hanteringen av skyddsvärd information
- behöver uppgifterna för sitt arbete

Fysiska handlingar ska hållas under god uppsikt eller förvaras inlåsta i säkerhetsskåp. Elektronisk förvaring ska ske så att endast behörig personal kan ta del av informationen, exempelvis genom behörighetsstyrning och åtkomst ska loggas. Informationen får inte lagras i datamedier utanför organisationens brandvägg/externt, till exempel på en privat dator eller i en molntjänst. Filer utan kryptering får inte förvaras lokalt på datorn, till exempel på skrivbordet . Informationen får inte förvaras i bil eller andra fordon utan uppsikt.

Kopiering eller utdrag ur handlingar ska ske i så liten omfattning som möjligt. För utskrift ska nätverksskrivare med behörighetsskyddad utskrift eller lokal skrivare inom synhåll från den som skriver ut dokumentet användas.

Information får inte delas utan kryptering via e-post eller andra icke-godkända fildelningsverktyg. För mer information om kryptering se bilaga 8 Skapa krypterade filer. Verktyget ”Skicka stora filer” med krav på inloggning med e-legitimation/mobilt bankID för att kunna ladda ner filerna får användas. Verktyget finns på https://filer.sundsvall.se För mer information om verktyget se Lathund – Hantera och skicka stora filer. Verktyget kan användas oavsett vem som är mottagare av informationen. Det är dock bara verksamheter och bolag inom Sundsvalls kommunkoncern som kan använda verktyget för att dela information.

För delning av information inom kommunkoncernen kan också information delas via det lokala nätverket genom att en mapp med begränsad behörighet upprättas på N: (gemensam).

Om informationen skickas via brev ska rekommenderat brev med säkerhetskuvert användas.

Möten och samtal där uppgifter i säkerhetsklass 3 diskuteras ska ske avskilt för att minska risken för att obehöriga tar del av informationen. Telefonsamtal bör undvikas.

Dokument ska förstöras med dokumentförstörare eller lämnas i ett låst kärl för destruktion.

4.5 Säkerhetsklass 4

4.5.1 Begränsat hemlig och konfidentiell information

Spridningen av informationen ska vara mycket starkt begränsad och enbart ske till personer som:

- bedöms pålitliga ur säkerhetssynpunkt
- har tillräckliga kunskaper om säkerhetsskydd

- behöver uppgifterna för sitt arbete
- är inplacerade i säkerhetsklass (ej krav vid begränsat hemlig information)

Fysiska handlingar, elektroniska handlingar, USB-minnen eller CD-skivor ska märkas med aktuell säkerhetsskyddsklass och diarienummer eller annan lämplig identifieringsuppgift.

Allmänna handlingar ska registeraras i diariet med en anteckning om var den förvaras, om den gallrats eller kommit bort. Handlingen ska dock inte läggas in digitalt i Public360 eller i något annat diarieföringssystem som inte godkänts av MSVA. Om handlingen inte längre bedöms vara säkerhetskyddsklassificerad eller om säkerhetskyddsklassen ändras ska detta noteras på handlingen, vem som fattat beslutet och datum. Är handlingen allmän ska ändringen också registreras i Public360.

Fysiska handlingar, elektroniska handlingar eller lagringsmedium ska förvaras inlåsta i säkerhetsskåp. Skyddsnivån ska motsvara lägst SS 3492. Övrig tid ska handlingarna vara under ständig uppsikt.

Uppgifterna får inte skickas med e-post eller lagras på datorer med möjlighet till internetanslutning, skrivas ut eller kopieras på nätverksskrivare eller delas muntligt via telefon.

Kopiering eller utdrag ska ske i så liten omfattning som möjligt. Vid delning av handlingar med säkerhetsskyddsklassificerade uppgifter ska delningen och mottagare registreras. Muntlig delgivning eller visning behöver inte registreras. Säkerhetsskyddsavtal (SUA) ska upprättas om information i säkerhetsskyddsklass konfidentiell eller högre delas inom ramen för ett affärsavtal.

I dagsläget har MSVA inte tillgång till signalskyddskrypto godkänt för att dela säkerhetsskyddsklassificerade uppgifter via datakommunikation eller via telefon. Handlingar ska därför överlämnas personligen, vilket är att föredra om det är möjligt, eller skickas som rekommenderat brev i ett säkerhetskuvert.

Kontrollera att säkerhetskuvertet inte är skadat, notera eller spara serienumret som finns på kuvertet och datum för när du skickar det samt mottagare för att möjliggöra spårning och verifiering. Kontakta gärna mottagaren innan informationen skickas för att utbyta information om serienummer och datum för distribution.

När du tar emot en försändelse i någon form av säkerhetsförslutet engångsemballage ska du undersöka att emballaget inte uppvisar spår av manipulation, till exempel i förslutning, skarvar och svetssömmar. Om spår av manipulation upptäcks eller om serienumret inte stämmer överens med det som avsändaren eventuellt angett ska det utredas som en potentiellt säkerhetshotande händelse. Kontakta vid behov säkerhetssamordnare.

Möten där uppgifter diskuteras ska ske i lokaler där riskreducerande åtgärder har vidtagits, exempelvis ska inga telefoner, läsplattor, datorer eller annan utrustning med möjlighet att ansluta till nätverk finnas i rummet.

Handlingar och datamedier som inte längre används, och inte ska arkiveras, ska destrueras. Handlingar ska brännas eller strimlas i en dokumentförstörare med lägst säkerhetsklass 5, spånstorlek 15x1,2 mm eller mindre. Handlingar får inte lämnas i de låsta kärl för destruktion som finns på MSVA.

4.5.2 Hemlig och kvalificerat hemlig information

För hemlig och kvalificerat hemlig information tillkommer ytterligare hanteringsregler. MSVA bedöms i nuläget inte hantera information i någon av dessa säkerhetsskyddsklasser, men det kan inte uteslutas att det vid något enstaka tillfälle kan bli aktuellt. I dessa fall är det VD som fattar beslut om förvaring av handlingar. Vid kopiering, utdrag eller vid medförande utanför våra lokaler krävs medgivande från VD. Förutom delning av handlingar och utdrag ska också muntlig delgivning eller visning av information registreras. Allmänna handlingar och lagringsmedier ska inventeras årligen. Destruktion ska dokumenteras.

7 Delning av information till andra aktörer

Att sekretess gäller för en uppgift innebär att det är förbjudet att röja uppgiften oavsett om det sker muntligen eller genom att en handling lämnas ut. Det kan dock finnas skäl och stöd i lagstiftningen att lämna ut en uppgift trots att den omfattas av sekretess.

7.1 Sekretessbrytande bestämmelser

I OSL finns det ett antal sekretessbrytande bestämmelser[2] som ger oss rätt att lämna ut sekretessbelagda uppgifter. Förutom ett antal paragrafer som berör specifika situationer finns också en generalklausul. Klausulen innebär att sekretessbelagda uppgifter får lämnas till en annan myndighet om det är uppenbart att intresset av att uppgiften lämnas ut har företräde framför det intresse som sekretessen ska skydda.[3] Sekretessbrytande bestämmelser kan också gälla vid absolut sekretess.

Offentligt anställda omfattas även av en grundlagsskyddad meddelarfrihet. Det innebär att offentligt anställda har rätt att muntligt lämna sekretessbelagda uppgifter till journalister eller författare för publicering om inte annat anges i OSL. I dessa fall får inte arbetsgivaren utreda vem som lämnat uppgifterna.

7.2 Inför delning av information till andra aktörer

7.2.1 Godtagbara skäl för att dela skyddsvärd information

När MSVA delar skyddsvärd information till externa aktörer ska informationen antingen vara en förutsättning för att företaget ska kunna utföra ett uppdrag/leverera en tjänst som vi har beställt eller för att en myndighet ska kunna utföra sin uppgift. Ett annat godtagbart skäl är att informationen utgör underlag för att ta fram obligatorisk statistik.

Ytterligare tillfälle där det kan finnas återkommande behov av att dela skyddsvärd information är när andra aktörer som infrastrukturägare, konsulter eller entreprenörer har behov av information om vårt ledningsnät för till exempel projektering, planering eller genomförande av projekt.

---

[2] Kap. 10 §§ 1-28 OSL
[3] Kap. 10 § 27 OSL

Om inte något av dessa skäl föreligger ska inte information i säkerhetsklass 2 eller högre delas, under förutsättning att ingen sekretessbrytande paragraf i OSL är tillämplig. Inför delning av information i säkerhetsklass 3 eller högre ska samråd ske med ansvarig chef på MSVA.

7.2.2 Delning till leverantörer

För att MSVA ska dela skyddsvärd information till leverantörer ska sekretess och/eller informationssäkerhet finns med i avtalet mellan MSVA och leverantören. I avtalet förbinder sig leverantören att följa våra hanteringsregler och, vid behov, våra krav på företagets arbete med informationssäkerhet. Det sistnämnda är aktuellt om företaget ska förvara och hantera information i säkerhetsklass 2 eller högre i sina lokaler och system.

För säkerhetsklass 2, 3 och 4 kan det också vara aktuellt att ställa krav på att företaget ska ha en säkerhetschef eller säkerhetsansvarig som kan vara vår kontaktperson i säkerhetsfrågor. Personen ska även ansvara för att genomföra säkerhetsprövningar av personer som ska delta i skyddsvärd verksamhet och/eller ta del av information samt för att berörda undertecknar en sekretessförbindelse. I de fall detta inte är lämpligt, till exempel vid avtal med fåmansföretag, genomförs detta i stället av MSVA.

För delning av information i säkerhetsklass 4 ska också krav på säkerhetsskydd ställas. I vissa fall kan det vara aktuellt att upprätta ett SUA-avtal mellan oss och leverantören. Med SUA-avtal avses säkerhetsskyddad upphandling med säkerhetsskyddsavtal som upprättas mellan oss och anbudsgivaren eller leverantören. Detta är ett krav enligt säkerhetsskyddslagen i de fall en upphandling omfattar säkerhetsskyddsklassificerade uppgifter på nivån konfidentiell eller högre och/eller innebär ett deltagande i säkerhetskänslig verksamhet på motsvarande nivå.

En upphandling och/eller ett avrop av en tjänst måste alltså föregås av en inventering och analys av vilken typ av information som leverantören kommer att ta del av inom ramen för uppdraget, i vilka säkerhetsklasser och om information i säkerhetsklass 2 eller högre ska förvaras i leverantörens lokaler/system eller inte. Inventeringen och analysen ligger till grund för kravställning gentemot leverantören vad avser sekretess, informationssäkerhet, säkerhetsprövningar och eventuell inplacering i säkerhetsklass.

De individer som ska ta emot skyddsvärd information i säkerhetsklass 2 eller högre ska ha undertecknat en sekretessförbindelse. Den som skriver under förbindelsen ska ha läst och förstått de hanteringsregler som gäller för den eller de säkerhetsklasser som är aktuella. För information om hanteringsregler till externa aktörer kan bilaga 6 Utdrag ur riktlinje Allmänna och säkerhetsklassade handlingar för information till leverantörer och andra externa intressenter

För säkerhetsklass 2, 3 och 4 ska också personen bedömas som pålitlig ur säkerhetssynpunkt. Säkerhetsprövningen ska anpassas till aktuell säkerhetsklass och i vilken omfattning personen kommer att ta del av skyddsvärd information. För säkerhetsklass 3 och 4 ska ett skriftligt intyg på godkänd säkerhetsprövning upprättas. Se bilaga 9 Information om säkerhetsprövning till leverantörer och andra externa intressenter för mer information .

För delning av information i säkerhetsklass 4 ska också mottagaren ha gått en utbildning i säkerhetsskydd. Krav på inplacering i säkerhetsklass gäller enbart om informationen i säkerhetsklass 4 har säkerskyddklassificering konfidentiell eller högre.

Vid SUA-avtal och delning av konfidentiell information ska mottagarna vara inplacerade i säkerhetsklass och ha genomgått en utbildning i säkerhetsskydd. I dessa fall är ett SUA-avtal en förutsättning både för att kunna dela information och för att kunna ställa krav på inplacering i säkerhetsklass.

7.2.3 Delning till myndigheter

Vid delning av information till myndigheter som omfattas av OSL kan vi inte avtala om hur informationen ska hanteras eller kräva att personer undertecknar en sekretessförbindelse. MSVA ska dock informera mottagaren om att vi bedömer att informationen är skyddsvärd och, i förekommande fall, om vilken paragraf i OSL som tillämplig samt vilka hanteringsregler vi förväntar oss att myndigheten ska följa. De personer som ska ta del av informationen ska ha kunskap om hantering av skyddsvärd och/eller sekretessbelagd information och bedömas vara pålitlig ur säkerhetssynpunkt. Myndighetens säkerhetschef eller säkerhetsskyddschef ska kontaktas vid behov för bedömning och intyg om godkänd säkerhetsprövning.

7.2.4 Delning av ledningsnätskartor utan affärsrelation

Även vid delning av ledningsnätskartor till aktörer som vi inte har någon egen affärsrelation till ska vi ställa krav på att mottagaren följer tillhörande hanteringsregler, att personer som tar del av information i säkerhetsklass 2 eller högre undertecknar sekretessförbindelser och bedöms pålitliga ur säkerhetsynpunkt. Är behovet av att ta del av ledningsnätskartor omfattande och/eller återkommande bör ett avtal som reglerar säkerhetskrav tecknas mellan MSVA och aktören. Vid övriga tillfällen ansvarar den som delar informationen för att kraven uppfylls. Kontakta säkerhetsamordnare vid behov av stöd.

7.3 Giltighetstid för sekretessförbindelser och intyg om säkerhetsprövning

Sekretessförbindelser och intyg om säkerhetsprövning kan antingen gälla för en ramavtalsperiod eller för ett enskilt uppdrag. För ramavtalsaktörer som återkommande genomför arbeten under hela avtalsperioden utan längre avbrott kan giltighetstiden anges till hela ramavtalsperioden, under förutsättning att angiven säkerhetsklass inte ändras eller att något som föranleder en ny säkerhetsprövning inte inträffar.

I de fall MSVA gör enstaka avrop för avgränsade uppdrag bör i stället sekretessförbindelser och intyg gälla för det aktuella uppdraget.

Kontakta säkerhetssamordnare vid behov av stöd i bedömningen av lämplig giltighetstid.

8 Brott mot tystnadsplikt och tjänstefel

Sekretess innebär att det är förbjudet att röja uppgiften oavsett om det sker muntligen eller genom att en handling lämnas ut. Den som röjer en sekretessbelagd uppgift kan dömas för brott mot tystnadsplikt under förutsättning att meddelarfrihet eller någon annan sekretessbrytande bestämmelse inte gäller. Detta gäller oavsett om det skett avsiktligt, på grund av slarv eller okunskap.

Den som medvetet eller av oaktsamhet sätter offentlighetsprincipen ur spel, exempelvis genom att vägra lämna ut offentliga handlingar, kan dömas för tjänstefel.

9 Bilagor

Bilaga 4 Sekretessförbindelse

Bilaga 8 Skapa krypterade filer

Bilaga 9 Information om säkerhetsprövning till leverantörer och andra externa intressenter