Informationssäkerhet – Lathund

Denna lathund beskriver hur vi på OKG hanterar information ur sekretessynpunkt. För komplett information, se instruktionerna 2011-02371 ”Regler för informations-säkerhet” och 2007-21444 ”Regler för IT-säkerhet”.

Sekretessklassificering

För att kunna uppnå hög informationssäkerhet sekretessklassas information. Sekretess-klassningen anger vilka krav som gäller för förvaring, distribution, destruktion m.m.

Behörig till att ta del av information är den som behöver informationen för att kunna genomföra sina arbetsuppgifter, är säkerhetsprövad, har tecknat tystnadsförbindelse och har tillräckliga kunskaper i informationssäkerhet/säkerhetsskydd.

Omklassificering av information på OKG

Omklassificering kan ske på uppdrag av informationsansvarig.

Utbyte av information med myndigheter

Svenska myndigheter tillämpar offentlighetsprincipen. Vid kontakt med myndighet ska begäran om vidmakthållande av sekretess ske utav dokument som klassificerats som intern med begränsad spridning, hemlig eller kvalificerat hemlig.

Utbyte av information med övriga externa parter

Vid utbyte av sekretessklassad information med extern part ska sekretessavtal och i vissa fall andra kompletterande avtal vara tecknat med denna.

OKGs interna regler för klassning, märkning, förvaring, distribution och destruktion ska användas som underlag vid framtagning av specifik rutin för hantering av OKG- information hos den externa parten.

USB-minnen - restriktiv hantering gäller, se 2007-21444 ”Regler för IT-säkerhet”.

Märkning

Märkning av dokument syftar till att ge en tydlig signal till mottagaren att särskilda hanteringsregler gäller. Märkningen har också en juridisk funktion då den avgör vilket lagrum som åberopas för att skydda innehållet mot obehörig spridning.

Information som nyproduceras eller uppdateras ska oberoende av sekretessklass, undantaget öppen, alltid märkas genom att använda mallar eller stämplar.

Dokumentation som sedan tidigare saknar märkning eller har annan märkning än den som framgår i 2011-02371 ”Regler för informationssäkerhet” ska stämplas med gällande märkning innan distribution utanför OKG.

Sekretessklassificering av information

Information ska alltid sekretessklassificeras och märkas då den skapas eller mottas.

Sekretessklasser

- **Öppen**
- **Intern**
- **Intern med begränsad spridning**
- **Hemlig (säkerhetsskyddsklass Begränsat hemlig)**
- **Kvalificerat hemlig (säkerhetsskyddsklass Konfidentiell)**

Öppen

Typ av information där spridning är önskvärd och begränsas inte av några krav på märkning, förvaring, distribution eller förstöring.

Intern

Typ av information där spridning, obehörig användning eller ändring av den skulle medföra begränsad eller mindre skada för företaget eller någon person.

Fysisk förvaring

Får förvaras öppet inom OKGs lokaler men skyddas mot obehöriga. Utanför OKG ska informationen hållas under uppsikt eller förvaras i låst utrymme.

Elektronisk förvaring

Informationen ska skyddas med hjälp av åtkomstkontroll och behörighetsstyrning.

Distribution

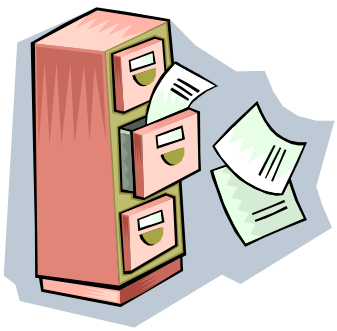
Får distribueras inom OKG. Extern distribution är tillåten ***om*** mottagaren är behörig.

Destruktion

Hanteras på OKG inom ordinarie pappersåtervinningssystem. Utanför OKG ska informationen destrueras så att obehörig spridning inte sker.

Elektronisk destruktion

För lagringsmedia där radering inte är möjlig, t ex cd/dvd, ska fysisk destruktion göras.



Intern med begränsad spridning

Typ av information som kan användas för informationshämtning inför ett sabotage, angrepp, terrorhandling eller stöld av kärnämne eller kärnavfall. Det är även sådan information som kan falla in under exportkontroll. Inkluderar bilder på tekniska installationer och utrustning på OKG. Utgångsläget för teknisk dokumentation är att den klassificeras som intern med begränsad spridning. Undantag finns där även sekretessklass intern eller öppen kan användas, se 2011-02371, ”*Regler för informationssäkerhet”*. Krävs starkare skydd klassificeras dokumentationen som hemlig eller kvalificerat hemlig.

Fysisk förvaring

Får förvaras öppet inom OKGs lokaler men skyddas mot obehöriga. Utanför OKG ska informationen hållas under uppsikt eller förvaras på ett betryggande sätt inom låst utrymme som skyddar mot obehörig åtkomst.

Elektronisk förvaring

Informationen ska skyddas med hjälp av åtkomstkontroll och behörighetsstyrning. Externt krävs att OKG gör en revidering av bolagets lokaler, IT- miljö etc. Användande av extern molntjänst för lagring är *inte* tillåtet.

Distribution

Får distribueras inom OKG. Extern distribution är tillåten ***om*** mottagaren är behörig. Informationen ska skickas som REK med tillägg mottagningskvittens/ mottagningsbevis alternativt som VÄRDE med tillägg mottagningskvittens. Försändelsen ska vara inslagen och förseglad på ett sådant sätt att man inte kan komma åt någon del av innehållet utan att göra fullt synliga skador på omslaget eller förseglingen. På OKG sker extern distribution inklusive bokföring och bevakning via Kontorsservice.

Elektronisk distribution

Extern distribution måste ske krypterat. OKG tillhandahåller två olika lösningar:

- Kryptering av filer/e-post (PGP, PKI, 7-Zip eller AxCrypt)
- Krypterad filservertjänst (secure FTP).

Destruktion

Hanteras på OKG inom ordinarie pappersåtervinningssystem. Utanför OKG ska informationen destrueras i dokumentförstörare med s k Cross Cut-funktion.

Elektronisk destruktion

För lagringsmedia där överskrivning med DBAN eller med annan av IT-säkerhetsansvarig godkänd metod inte är möjlig, t ex cd/dvd, ska fysisk destruktion göras.

Hemlig

Typ av information som ger företaget en klar fördel framför sina konkurrenter och vars avslöjande, spridning, användning eller ändring skulle kunna medföra skadeverkningar för företaget eller någon person. Hemlig information omfattar även uppgifter i säkerhetsskyddsklassen begränsat hemlig vilka kan medföra ringa skada för Sveriges säkerhet vid ett röjande.

Fysisk förvaring

Ska förvaras i säkerhetsskåp, inbrottsskyddat datamediaskåp, värdeskåp som är klassat enligt inbrottsklass SS 3492 alternativt SSF 3492 eller inbrottsskyddat arkiv.

Elektronisk förvaring

Hanteras i separat säkerhetsnät. Åtkomst till applikation ska ske via 2-faktorsinloggning. Utskrift är tillåten till speciella skrivare som kräver personlig identifiering innan start av utskrift. Revidering av nätet ska ske. Externt krävs att OKG gör en revidering av bolagets lokaler, IT- miljö etc.

Distribution

På OKG sker fysisk distribution genom personlig överlämning. Extern distribution är tillåten ***om*** mottagaren är behörig. Informationen ska skickas som REK med tillägg mottagningskvittens/ mottagningsbevis alternativt som VÄRDE med tillägg mottagningskvittens. Försändelsen ska vara inslagen och förseglad på ett sådant sätt att man inte kan komma åt någon del av innehållet utan att göra fullt synliga skador på omslaget eller förseglingen. På OKG sker extern distribution inklusive bokföring och bevakning via Kontorsservice. Innan distribution utomlands ska informationssäkerhets-ansvarig kontaktas för bedömning om distributionen är tillåten enligt gällande lagstiftning samt för riskbedömning av valt distributionssätt.

Delgivning till behörig mottagare som inte finns på ursprunglig distributionslista ska godkännas av utfärdare (förutsatt att personen har samma ansvarsområde) alternativt informationsansvarig och bokföras genom uppdatering av distributionslistan.

Elektronisk distribution

Internt OKG sker distribution i första hand via applikation benämnd hemliga Oden. Distribution får ske på CD,DVD eller OKG godkänt USB-minne, regler för fysisk distribution enligt ovan ska tillämpas. Informationen får inte diskuteras på telefon.

Destruktion

Destrueras i dokumentförstörare med s k Cross Cut-funktion.

Elektronisk destruktion

För lagringsmedia där överskrivning med DBAN eller med annan av IT-säkerhetsansvarig godkänd metod inte är möjlig, t ex cd/dvd, ska fysisk destruktion göras.

Kvalificerat hemlig

Omfattar uppgifter i säkerhetsskyddsklassen konfidentiell, vilka kan medföra en inte obetydlig skada för Sveriges säkerhet vid ett röjande. Förvaring sker hos OKGs säkerhetsskyddschef.