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.

OKG kan endast kräva att andra företag och myndigheter samt enskilda ska skydda vår information om den är klassificerad av oss.

Behörig att ta del av information, undantaget sekretessklass öppen, är den som behöver informationen för att kunna genomföra sina arbetsuppgifter, är säkerhetsprövad och har tecknat tystnadsförbindelse.

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 vara tecknat. Vidare ska hanteringsregler finnas som beskriver ansvar och aktiviteter både vid mottagandet och vid sändandet av information på olika media. Syftet är att säkerställa bevarande av sekretess både för extern part och OKG.

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.

Hantering av befintlig teknisk dokumentation med sekretessklasserna intern samt intern med begränsad spridning, som sedan gammalt inte är märkt, ska genom kunskap vara känd.

Sekretessklassificering av information

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

Sekretessklasser

- **Öppen**
- **Intern**
- **Intern med begränsad spridning**
- **Hemlig**
- **Kvalificerat hemlig**

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

Ska ske kontrollerat så att endast behörig personal kan ta del av informationen.

Distribution

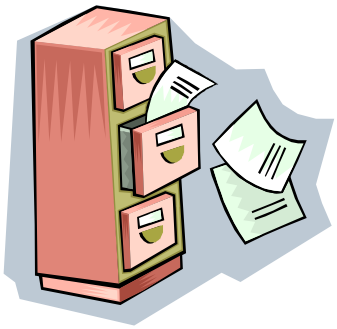
Får distribueras inom OKG. Extern distribution är tillåten ***om*** mottagaren är behörig.

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. Detta inkluderar även 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 förvaras på ett betryggande sätt inom låst utrymme som skyddar mot obehörig åtkomst.

Elektronisk förvaring

Externt krävs att OKG gör revidering av bolagets it-miljö med avseende på informations- och it-säkerhet som ska godkännas på beslutsmöte informations- och it-säkerhet.

Distribution

Får distribueras inom OKG. Extern distribution är tillåten ***om*** mottagaren är behörig. Informationen ska skickas som ”Brev med tilläggstjänst – Rek alternativt Värde” med mottagningsbevis/ mottagningskvittens, enligt PostNord Sverige ABs villkor. På OKG sker extern distribution inklusive bokföring och bevakning via Kontorsservice.

Elektronisk distribution

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

- krypterad e-postlösning
- krypterad filservertjänst

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 radering 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 med betydelse för rikets säkerhet.

Fysisk förvaring

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

Elektronisk förvaring

Hanteras i separat säkerhetsnät som är väl avgränsat från övriga it-system. Åtkomst till applikation ska ske via 2-faktorsinloggning. Utskrift är tillåten till speciella skrivare som kräver personlig identifiering innan start av utskrift. OKG ska göra revidering av nätet som ska godkännas på beslutsmöte informations- och it-säkerhet.

Distribution

Får skickas via OKGs internpost med följande krav:

- Informationen ska stoppas i ett förseglat och adresserat kuvert.
- Kuvertet ska sedan stoppas i ett cirkulationskuvert.
- Avsändaren ska förvissa sig om att mottagaren är på plats innan försändelsen skickas och informera om att försändelsen är på väg.
- Avsändaren ska dokumentera mottagarens namn, avsändardatum och informationens registreringsnummer eller motsvarande. Informationen sparas tills avsändaren försäkrat sig om att informationen nått mottagaren.
- Mottagaren ska bekräfta att informationen kommit fram.

Om inte kvittens på skickad information har erhållits hos avsändaren inom en vecka ska detta anmälas till informationssäkerhetsansvarig som gör en bedömning avseende skada.

Extern distribution är tillåten ***om*** mottagaren är behörig. Informationen ska skickas som ”Brev med tilläggstjänst – Rek alternativt Värde” med mottagningsbevis/ mottagningskvittens, enligt PostNord Sverige ABs villkor. På OKG sker extern distribution inklusive bokföring och bevakning via Kontorsservice.

Delgivning till mottagare som inte finns på ursprunglig distributionslista, ska godkännas av informationsansvarig och bokföras av enheten för informationshantering på OKG.

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 bör inte diskuteras på telefon.

Destruktion

Destrueras i dokumentförstörare med s k Cross Cut-funktion.

Elektronisk destruktion

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

Kvalificerat hemlig

Typ av information som omfattar uppgifter av synnerlig betydelse för rikets säkerhet och information som behöver hållas hemliga med hänsyn till Unipers framtida marknadspositioner. Förvaring sker hos OKGs säkerhetsskyddschef.