Rutin för informationsklassning, märkning och hantering

Version 1.2 Datum 220203

Författare Erik Bolinder, informationssäkerhetssamordnare Klick Data AB (publ)

Godkänd av Ulrika Bolinder, ordförande Klick Data AB (publ)

Klassificering Publik Version Datum Beskrivning 1.0 2018-10-17 Godkänd

Roller och ansvar

Informationssäkerhetssamordnare ansvarar för att detta dokument är aktuellt och relevant.
VD är ytterst ansvarig för efterlevnad av den här rutinen.

Alla anställda ansvarar för att denna rutin följs för alla dokument som omfattas av Klick Datas ledningssystem för informationssäkerhet.

Syfte

Rutin för informationsklassning, märkning och hantering beskriver företagets modell för informationsklassning, rutiner för märkning samt regler för hantering av information i de olika klasserna. Rutinen följer ISO 27001.

Omfattning

Den här rutinen omfattar hela företaget, ingående IT-komponenter, företagets anställda, leverantörer och externa parter.

Referensdokument ISO/IEC 27001: 2005 Information Security Management Systems - Requirements

Definitioner Inga

Innehållsförteckning

1 Modell för informationsklassning

1.1 Allmänt

Följande riktlinjer består dels av den regeltext som återfinns i ”Regler för IT-säkerhet vid Klick Data” och dels av riktlinjer i form av tillägg, exempel och förslag som ska ses som god praxis vid informationsklassning. Information i alla dess former är en viktig tillgång för Klick Data AB (publ) (KD).

Att klassa informationen är grundläggande för att ge den nödvändigt och tillräckligt skydd. Utvecklingen inom IT gör det möjligt att hantera (skapa, lagra, utbyta och förmedla) information elektroniskt i allt större utsträckning.

Att klassa den information som hanteras underlättar bedömningen av vilka elektroniska hjälpmedel eller tjänster som kan nyttjas. Klassificeringsmodellen baseras på de, enligt SS-ISO/IEC 27001, **tre vedertagna informationssäkerhetsaspekterna: konfidentialitet, riktighet och tillgänglighet**.

Därutöver finns möjligheten att lägga till aspekter (till exempel spårbarhet, avbrottsskydd, icke-förnekbarhet) där speciella krav på informationssäkerhet föreligger. Behandling av information som innehåller personuppgifter ska anmälas till företagets personuppgiftsombud som ger anvisningar om hur informationen får hanteras.
Se https://klickdata.se/gdpr

Informationsägaren är ansvarig för informationsklassning av sin information samt att klassificeringen genomförs utifrån kriterierna konfidentialitet, riktighet och tillgänglighet. Följande uppställning ger exempel på vem som äknas som informationsägare i olika fall om inget annat beslutats.

Kategori Ägare (om ej annat anges)
Den som fastställt dokumentet Fastställda dokument
Objektsägare, objektsledare eller motsvarande Data i informationssystem
Utfärdaren All annan information

1.2 Användningsområden

Konkreta användningsområden där en informationsklassificering bör ligga till grund för val av säkerhetsnivå och därav följande säkerhetsåtgärder är:

- vid kravställning/kravspecificering inför systemutveckling eller upphandling av system,
- när säkerhetsdesign av ett informationssystem fastställs,
- när risk- och hotbildsanalyser av ett systemförvaltningsobjekt eller enskilt informationssystem genomförs,
- när informationssäkerhetsanalyser (egenkontroller) i ett förvaltningsobjekt eller enskilt informationssystem genomförs,
- när hanteringsregler av information, till exempel. med avseende på krav på kryptering av epost, regler för och eventuell märkning av intern och extern post eller kommunikation via mobiltelefon, fastställs.

SÄKERHETSNIVÅER

Klassificeringen görs med utgångspunkt i omfattningen av de konsekvenser som kan uppkomma vid brister i skyddet. Behovet av säkerhet (skyddsbehovet) för information beskrivs med någon av följande

nivåer: klass 1, klass 2 eller klass 3. Publik information, som till exempel information nedladdad från internet eller allmänt tillgänglig text eller bild, behöver inte alls klassificeras. Man kan uttrycka det som att det finns ytterligare en nivå, ”publik”, utan något specificerat behov av säkerhet. Behov av säkerhetsnivå beskrivs separat för var och en av de tre säkerhetsaspekterna nedan.

1.3 Kriterier för informationsklassning

Informationsklassning ska säkerställa att informationen får en lämplig skyddsnivå. Som utgångspunkt används kriterierna konfidentialitet, riktighet och tillgänglighet.

Med konfidentialitet avses att informationen inte får göras tillgänglig eller avslöjas för obehöriga.

Med riktighet avses att informationen inte ska kunna förändras och förvanskas av misstag eller av någon obehörig. I riktighet ingår spårbarhet, det vill säga att informationen och förändringar av denna ska kunna härledas till den som skapat informationen.

Med tillgänglighet avses att informationen ska finnas till hands för behöriga användare vid behov. De tre huvudkriterierna ska tas med i bedömningen för att avgöra nivån för skyddet av den aktuella informationen eller IT-systemet.

2 Beskrivning av säkerhetsklasserna

2.1 Konfidentialitet

Konfidentialitet handlar om behovet av skydd mot att informationen görs tillgänglig eller avslöjas för obehöriga personer, system eller processer.

Klass 1

Allmän beskrivning
Information som behöver skydd mot oavsiktlig eller obehörig åtkomst. Informationen kan avsiktligt göras tillgänglig för allmänheten. Exempel på information Merparten av informationen vid företaget (arbetsmaterial, men även allmänna handlingar) ingår i klass 1. Exempel på skydd Informationen ska vara skyddad mot oavsiktlig eller obehörig åtkomst genom inloggning, inlåsning eller på annat sätt skyddad förvaring. Offentlig information ska vara tillgänglig på ett kontrollerat sätt. Möjliga konsekvenser av brister Brister i skyddet kan medföra obehag eller begränsad ekonomisk förlust för enskilda eller begränsad skada för företaget eller tredje part.

Klass 2

Allmän beskrivning
Information som behöver ett starkare skydd mot oavsiktlig eller obehörig åtkomst inklusive information som ska hanteras med försiktighet. Exempel på information Personuppgifter inklusive personnummer, information med upphandlingssekretess och liknande. Exempel på skydd Informationen ska vara skyddad genom hårddiskkryptering, lösenordsskydd, inlåsning i väl skyddat skåp eller motsvarande skyddsgrad, som är godkänd enligt företagets avtal. Möjliga konsekvenser av brister Brister i skyddet kan

orsaka omfattande obehag eller ekonomisk förlust för enskilda eller omfattande skada för företaget eller tredje part.

Klass 3

Allmän beskrivning
Information som behöver ett särskilt starkt skydd mot oavsiktlig eller obehörig åtkomst, inklusive skydd mot kvalificerade angrepp avsedda att komma åt informationen. Exempel på information Sekretesskyddad information, starkt integritetskänslig information (till exempel känsliga personuppgifter som uppgifter om hälsotillstånd). Exempel på skydd Informationen ska vara skyddad genom kvalificerad kryptering vid överföring. Vid förvaring ska informationen skyddas genom stark autentisering och inlåsning i väl skyddat skåp eller motsvarande. Möjliga konsekvenser av brister Brister i skyddet kan medföra skada på liv eller hälsa för enskilda, orsaka omfattande obehag eller ekonomisk förlust för ett stort antal personer eller mycket allvarligt skada företaget eller tredje part.

2.2 Riktighet

Behovet av skydd mot att informationen förändras eller förstörs obehörigen, av misstag eller på grund av funktionsstörningar.

Klass 1

Allmän beskrivning
Information som behöver ett grundläggande skydd mot att förändras eller förstöras. Exempel på information Merparten av informationen vid företaget (arbetsmaterial och allmänna handlingar) ingår i klass 1. Exempel på skydd Informationen ska vara skyddad mot oavsiktlig eller obehörig förändring eller förstöring exempelvis genom säkerhetskopiering, noggrann testning av program, skyddad förvaring eller signatur på dokument. 6 (14) Möjliga konsekvenser av brister Brister i skyddet kan medföra obehag eller begränsad ekonomisk förlust för enskilda eller begränsad skada för företaget eller tredje part.

Klass 2

Allmän beskrivning
Information som behöver ett starkt skydd mot att förändras eller förstöras. Exempel på information Beslut och annan information som har ”rättsverkan” eller som har stor betydelse för företaget eller enskilda. Exempel är bokföringsmaterial, information i bokförings- och redovisningssystem, listor med tentamensresultat och forskningsdata med stor vetenskaplig eller ekonomisk betydelse. Exempel på skydd Informationen ska vara väl skyddad mot oavsiktlig eller obehörig förändring eller förstöring, exempelvis genom loggning av förändringar, digitala signaturer, manuella signaturer och noggranna hanteringsrutiner. Möjliga konsekvenser av brister Brister i skyddet kan orsaka omfattande obehag eller ekonomisk förlust för enskilda eller omfattande skada för företaget eller tredje part.

Klass 3

Allmän beskrivning

Information som behöver ett särskilt starkt skydd mot att förändras eller förstöras. Exempel på information Original till avhandlingar, Ladok databasens tabeller över personer och deras studieresultat, avtalsoriginal samt känsliga personuppgifter. Exempel på skydd Mycket kvalificerat skydd mot oavsiktlig och obehörig förändring, till exempel genom användning av certifikatbaserade digitala signaturer och kontrollsummor. Särskilt utformade rutiner för säkerhetskopiering och loggning av förändringar. Möjliga konsekvenser av brister Brister i skyddet kan medföra skada på liv eller hälsa för enskilda, orsaka omfattande obehag eller ekonomisk förlust för ett stort antal personer, eller mycket allvarligt skada företaget eller tredje part.

2.3 Tillgänglighet

Behovet av skydd som möjliggör att informationen är åtkomlig och användbar på förväntat sätt och inom önskad tid. Klass 1 Allmän beskrivning Information som normalt ska vara tillgänglig dygnet runt (eller vid särskilt beslutade tider), men där enstaka avbrott upp till en halv arbetsdag endast medför begränsad skada.

Exempel på information

Merparten av informationen vid företaget (arbetsmaterial och allmänna handlingar av i första hand internt intresse) ryms inom klass 1. Exempel på skydd Informationen ska helst vara tillgänglig hela dygnet. Informationens tillgänglighet ska möjliggöras genom stabila och väl testade IT-system och fungerande stödrutiner. Möjliga konsekvenser av brister Brister i tillgängligheten kan medföra obehag eller begränsad ekonomisk förlust för enskilda eller begränsad skada för företaget eller tredje part.

Klass 2

Allmän beskrivning
Information som ska vara tillgänglig dygnet runt (eller vid särskilt beslutade tider) utan avbrott. Enstaka kortare avbrott medför endast begränsad skada. Exempel på information Företagets externa webbsidor, information som studenter behöver för att fullgöra studier eller tentamina (till exempel information om tider och lokaler), gemensamma e-postsystem, information på filservrar samt allmänna handlingar av stort intresse för allmänheten. Exempel på skydd Informationen ska vara tillgänglig under hela dygnet. Planerade avbrott ska aviseras i god tid. Möjliga konsekvenser av brister Brister i tillgängligheten kan orsaka omfattande obehag eller ekonomisk förlust för enskilda eller omfattande skada för företaget eller tredje part.

Klass 3

Allmän beskrivning
Information som måste vara tillgänglig dygnet runt (eller vid särskilt beslutade tider) utan avbrott, och där även kortare avbrott kan orsaka stor skada. Exempel på information Katalog- och inloggningstjänster (informationen i dessa), DNS, DHCP och andra tjänster av mycket stor betydelse för utnyttjandet av samtliga IT-tjänster vid företaget. Exempel på skydd Redundanta system och andra åtgärder för att möjliggöra i princip obruten åtkomst trots mycket allvarliga störningar (till exempel redundanta system i olika lokaler). Möjliga konsekvenser av brister Brister i tillgängligheten kan medföra skada på liv eller hälsa för enskilda, orsaka omfattande obehag eller ekonomisk förlust för ett stort antal personer, eller mycket allvarligt skada företaget eller tredje part.

Särskilda krav på säkerhet

Det finns en mindre mängd information som på grund av sitt skyddsvärde kan hamna utanför detta dokuments tre klasser. Denna typ av information kan inte hanteras inom företagets standardutbud av säkerhets- och IT-tjänster utan måste analyseras i varje enskilt fall och en anpassad lösning måste tas fram. Säkerhetsfunktionen och IT-enheten kan vara behjälpliga i detta arbete.

Exempel på information
Exempel på skydd Skyddade identiteter eller adresser, särskilt känslig forskningsinformation, stora mängder särskilt känsliga personuppgifter (exempelvis journaler inom psykiatrivården) samt information som omfattas av försvarssekretess. Mycket kvalificerat skydd mot obehörig eller oavsiktlig åtkomst. Det ska finnas skydd mot kvalificerade angrepp avsedda att komma åt informationen.

3 Märkning

När information fått sin klassificering ska följande riktlinjer gälla för märkning:

För elektroniska och pappersbaserade dokument, använd utrymmet inom sidhuvudet och sidfoten inklusive första sidan.

Använd större, hårdare text än huvudtexten.

Använd dessutom klassificeringsetiketten längst upp på alla täckningsbrev och flagga e-postmeddelanden.

För datormedia, till exempel skivor, band, CD-skivor och DVD-skivor, se till att en lämplig, fast bifogad etikett tydligt anger klassificeringen.

För pappersfiler/mappar som innehåller pappersbaserade dokument (adresseras i första punkten ovan), använd klassificeringsetiketten på framsidan så att den tydligt visas. I sådana fall måste klassificeringsnivån för hela mappen/filen sättas till den högsta klassificeringsnivån som finns i materialet.

Varje sida i en fil/mapp måste uppfylla de krav som anges ovan för elektroniska och pappersbaserade dokument.

4 Hantering

4.1 Sammanfattning

Resultatet av klassificeringen ska ligga till grund för nivån på skyddet av den aktuella informationen eller IT-systemet. Resultatet utgör även grund för hur informationsägaren ska hantera informationen och underlag för systemägarens kravställning på ett IT-system. Klassning av information kan också ändras över tid. Exempel på det är vid upphandling då anbudssekretess råder ända fram till dess att val av leverantör är klart.

Tabellen nedan visar vilket skydd som krävs för en specifik klassning i ett visst sammanhang

	Klass 3	Klass 2	Klass 1
Bakgrundskontroll av personal	Bakgrundkontroller måste utföras för personal som behöver tillgång till information med särskilda krav på säkerhet.	Bakgrundkontroller måste utföras för personal som behöver tillgång till information som kräver hög säkerhet.	Bakgrundkontroller bör utföras för personal som behöver tillgång till information på basnivå.
Behörighet och åtkomst	All åtkomst till information med särskilda krav på säkerhet måste loggas. Detta inkluderar misslyckade försök till åtkomst och läsåtkomst. Varje loggrad ska identifiera användaren som sökt åtkomst, vilken information som eftersökts, tid datum och om åtkomst lyckats eller inte.	All tillgång till konfidentiell information ska loggas. Varje loggrad ska identifiera användaren som sökt åtkomst.	Loggning är inte nödvändig.

	Klass 3	Klass 2	Klass 1
Destruering av papper	Destruering sker genom godkänd malning, pulverisering, bränning eller omvandling till massa av en betrodd godkänd person eller organisation. Destrueringen måste registreras.	Destruering sker genom strimling. Alternativt kan konfidentiellt material kasseras i godkända konfidentiella avfallshanteringsfack.	Destruering sker genom strimling.
Destruktion av digital information	Vid byte av hårddisk ska den utbytta hårddisken förstöras mekaniskt så att lagrad information inte kan återskapas. Destruktionsintyget ska arkiveras.	Vid byte av hårddisk ska den utbytta hårddisken förstöras mekaniskt alternativt skrivas över enligt standard DoD 5520-22 med ett överskrivningsprogram så att lagrad information inte kan återskapas. Överskrivningsprogrammet tillhandahålls av universitetet. Destruktionsintyg respektive signerad anteckning om överskrivning ska arkiveras.	Vid byte av hårddisk ska den utbytta hårddisken förstöras mekaniskt alternativt skrivas över enligt standard DoD 5520-22 med ett överskrivningsprogram så att lagrad information inte kan återskapas. Överskrivningsprogrammet tillhandahålls av universitetet.
Digital överföring av	Information får endast skickas till auktoriserade	Information får endast skickas till auktoriserade	Inga restriktioner.

	Klass 3	Klass 2	Klass 1
Fax	Får inte användas. Risker för att använda faxapparater inkluderar: 1. Obehörig åtkomst till inbyggd minnesmedia för att hämta meddelanden; 2. Avsiktlig eller oavsiktlig programmering av maskiner för att skicka meddelanden till specifika nummer; 3. Dokument och meddelanden kan skickas till fel nummer, antingen genom att fel nummer slås in eller genom att nummer är felaktigt lagrade.	Avsändaren måste se till att destinationen är korrekt och att tillräckliga säkerhetsåtgärder finns på mottagningsplatserna. Mottagare måste omedelbart bekräfta mottagandet av ett faxmeddelande.	Inga restriktioner
Hantering och lagring av papper och andra flyttbara lagringsmedier	Informationen får lagras på annat flyttbart lagringsmedium under förutsättning att hela mediet är krypterat samt att det förvaras inlåst i säkerhetsskåp av klass SS3492 när det inte används. Det flyttbara mediet får inte lämnas utan uppsikt och inte heller flyttas utanför GU:s lokaler såvida det inte skickas till annan behörig mottagare.	Får hanteras inom en fysiskt säker miljö, exempelvis en inte offentlig kontorsmiljö. Se till att obehöriga inte kan se informationen. Mediet måste låsas undan när det inte används.	Se till att obehöriga inte kan se informationen. Mediet måste förvaras säkert när det inte används.
Kopiering av information	Kopiering måste godkännas av informationsägaren. Det måste finnas strikt kontroll över kopieringen med särskilda krav på säkerhet. Dokument måste kontrolleras och loggas. Eventuella extra eller onödiga kopior måste destrueras på säkert sätt. I förekommande fall måste originalhandlingar märkas med "YTTERLIGARE KOPIERING INTE TILLÅTEN".	Kopiering måste utföras eller övervakas av betrodda personer. Eventuella extra eller onödiga kopior måste förstöras.	Inga begränsningar.

	Klass 3	Klass 2	Klass 1
Publika nätverk, inklusive internet	Direkta anslutningar från publika nätverk är inte tillåtna. Anslutningar måste göras via en DMZ implementerad med en säker brandvägg.	Direkta anslutningar från publika nätverk är inte tillåtna. Anslutningar måste göras via en DMZ implementerad med en säker brandvägg.	Anslutningar måste göras via en godkänd säker brandvägg.
Regel om städat skrivbord	Allt material måste låsas in när det inte används, till exempel i ett godkänt säkerhetsskåp.	Allt material måste låsas in när det inte används.	Allt material måste förvaras säkert när det inte används.
Spårbarhet	Varje inmatning (transaktion) eller förändring av information ska vara spårbar och riktigheten för varje inmatning eller förändring av informationen ska kunna verifieras. Informationen ska förses med ett högt skydd mot oavsiktlig eller avsiktlig förändring och får endast hanteras i ett skyddat nät med ett anpassat behörighetskontrollsystem. Informationen får inte lagras i eller synkroniseras med en molntjänst. Upphandlade tjänster som uppfyller kraven på verifiering av transaktioner är undantagna.	Informationen ska vara spårbar och riktigheten ska kunna verifieras till exempelgenom signering.	Spårbarhet är inte nödvändig.
Tele-, video- och webbkonferens	Mottagarens identitet måste bekräftas och försiktighetsåtgärder vidtas för att förhindra avlyssning. Samtal får endast ske där man kan försäkra sig om att det inte finns någon risk för att det avlyssnas, antingen direkt eller med övervakningsteknik.	Mottagarens identitet måste bekräftas och försiktighetsåtgärder vidtas för att förhindra avlyssning. Lämna inte meddelanden innehållande information av hög säkerhetsnivå på telefonsvarare eftersom de kan spelas upp av obehöriga personer, lagras på kommunala system eller lagras felaktigt till följd av felringning.	Inga restriktioner.

	Klass 3	Klass 2	Klass 1
Lagring av digital information	Informationen ska lagras på fristående server i isolerat nät och inte på arbetsstationens lokala hårddisk. Servern ska vara placerad i ett godkänt låst serverrum I de fall då en server inte finns att tillgå ska informationen lagras på en krypterad separat hårddisk som när den inte används ska förvaras i ett säkerhetsskåp av klass SS 3492. Bärbar dator låses in, på motsvarande sätt, då den inte används. Åtkomst till information måste skyddas med stark autentisering.	Informationen ska lagras på en fristående server i ett skyddat nät. Servern ska vara placerad i ett godkänt serverrum. Informationen får i undantagsfall lagras på en arbetsstation under förutsättning att hela lagringsmediet är krypterat och att IT-systemet inte delar ut resurser. Informationen får inte lagras i eller synkroniseras med en extern molntjänst.	Informationen ska i första hand lagras på en fristående server och inte på arbetsstationens lokala hårddisk. Servern ska vara placerad i ett godkänt serverrum. Lagring i och synkronisering med molntjänster som tillhandahålls av GU är tillåten.
Mobila medier	Informationen får lagras på flyttbart lagringsmedium under förutsättning att hela mediet är krypterat samt att det hålls inlåst när det inte används. Dessa medier får inte lämnas utan uppsikt och inte heller flyttas utanför universitetets lokaler såvida det inte skickas till annan behörig mottagare. Åtkomst till information måste skyddas med stark autentisering.	Data måste krypteras. Mobila medieenheter, inklusive bärbara datorer, får inte lämnas obevakade och måste förvaras inlåsta när de inte används. Åtkomst till information måste skyddas med ett säkert lösenord.	Mobila medieenheter, inklusive bärbara datorer, får inte lämnas obevakade och måste förvaras inlåsta när de inte används. Åtkomst till information måste skyddas med ett säkert lösenord.
Muntliga samtal	Muntliga samtal får endast ske där man kan försäkra sig om att det inte finns någon risk för att konversationer avlyssnas, antingen direkt eller med övervakningsteknik.	Muntliga samtal får inte äga rum på en allmän plats eller där de kan avlyssnas.	Muntliga samtal får inte äga rum där de kan avlyssnas.
Post	Information får endast skickas till auktoriserade mottagare. Informationen får inte sändas med internpost utan ska överlämnas personligen eller med bud. Vid försändning externt ska postbefordran med REK och mottagningsbevis alternativt bud användas.	Information får endast skickas till auktoriserade mottagare. Leverans får ske med godkänt bud eller annan leveransmetod som kan spåras. Vid försändning med internpost ska dubbla förslutna kuvert användas. Vid försändning externt ska postbefordran med REK och mottagningsbevis alternativt bud användas.	Information får endast skickas till auktoriserade mottagare. Vid försändning med internpost ska förslutet kuvert användas. Extern posthantering får användas.

Klass 3 Klass 2 Klass 1 Bakgrundskontroll av personal Bakgrundkontroller måste utföras för personal som behöver tillgång till information med särskilda krav på säkerhet. Bakgrundkontroller måste utföras för personal som behöver tillgång till information som kräver hög säkerhet. B akgrundkontroller bör utföras för personal som behöver tillgång till information på basnivå. Behörighet och åtkomst All åtkomst till information med särskilda krav på säkerhet måste loggas. Detta inkluderar misslyckade försök till åtkomst och läsåtkomst. Varje loggrad ska identifiera användaren som sökt åtkomst, vilken information som eftersökts, tid datum och om åtkomst lyckats eller inte. All tillgång till konfidentiell information ska loggas. Varje loggrad ska identifiera användaren som sökt åtkomst. Loggning är inte nödvändig.
Klass 3 Klass 2 Klass 1 Destruering av papper Destruering sker genom godkänd malning, pulverisering, bränning eller omvandling till massa av en betrodd godkänd person eller organisation. Destrueringen måste registreras. Destruering sker genom strimling. Alternativt kan konfidentiellt material kasseras i godkända konfidentiella avfallshanteringsfack. Destruering sker genom strimling. Destruktion av digital information Vid byte av hårddisk ska den utbytta hårddisken förstöras mekaniskt så att lagrad information inte kan återskapas. Destruktionsintyget ska arkiveras. Vid byte av hårddisk ska den utbytta hårddisken förstöras mekaniskt alternativt skrivas över enligt standard DoD 5520-22 med ett överskrivningsprogram så att lagrad information inte kan återskapas. Överskrivningsprogrammet tillhandahålls av företaget. Destruktionsintyg respektive signerad anteckning om överskrivning ska arkiveras. Vid byte av hårddisk ska den utbytta hårddisken förstöras mekaniskt alternativt skrivas över enligt standard DoD 5520-22 med ett överskrivningsprogram så att lagrad information inte kan återskapas. Överskrivningsprogrammet tillhandahålls av företaget. Digital överföring av information Information får endast skickas till auktoriserade mottagare och måste vara krypterad till lämplig nivå. Endast säkra protokoll (till exempel. TLS, SSLv3) ska användas. Osäkra protokoll som ftp och telnet ska inte användas. Information får endast skickas till auktoriserade mottagare. Extern överföring är endast tillåten om data överförs skyddad med stark kryptering. Överväg att använda säkra protokoll (till exempel TLS, SSLv3). Osäkra protokoll som ftp och telnet ska inte användas. Inga restriktioner. E-post Information

får endast skickas till auktoriserade mottagare och måste vara krypterad till lämplig nivå. Information får endast skickas till auktoriserade mottagare. Extern epost är endast tillåten om data överförs skyddad med stark kryptering. Inga restriktioner. Extern åtkomst Är inte tillåtet, om inte specifikt godkänt av säkerhetschefen. Alla kontroller och restriktioner som beskrivs ovan ska tillämpas. Endast tillåtet när det specifikt godkänts av närmsta chef. Alla kontroller och restriktioner som beskrivs ovan ska tillämpas. Alla kontroller och restriktioner som beskrivs ovan ska tillämpas.

Fax Får inte användas. Risker för att använda faxapparater inkluderar: 1. Obehörig åtkomst till inbyggd minnesmedia för att hämta meddelanden; 2. Avsiktlig eller oavsiktlig programmering av maskiner för att skicka meddelanden till specifika nummer; 3. Dokument och meddelanden kan skickas till fel nummer, antingen genom att fel nummer slås in eller genom att nummer är felaktigt lagrade. Avsändaren måste se till att destinationen är korrekt och att tillräckliga säkerhetsåtgärder finns på mottagningsplatserna. Mottagare måste omedelbart bekräfta mottagandet av ett faxmeddelande. Inga restriktioner Hantering och lagring av papper och andra flyttbara lagringsmedier Informationen får lagras på annat flyttbart lagringsmedium under förutsättning att hela mediet är krypterat samt att det förvaras inlåst i säkerhetsskåp av klass SS3492 när det inte används. Det flyttbara mediet får inte lämnas utan uppsikt och inte heller flyttas utanför KD:s lokaler såvida det inte skickas till annan behörig mottagare. Får hanteras inom en fysiskt säker miljö, exempelvis en inte offentlig kontorsmiljö. Se till att obehöriga inte kan se informationen. Mediet måste låsas undan när det inte används. Se till att obehöriga inte kan se informationen. Mediet måste förvaras säkert när det inte används. Kopiering av information Kopiering måste godkännas av informationsägaren. Det måste finnas strikt kontroll över kopieringen med särskilda krav på säkerhet. Dokument måste kontrolleras och loggas. Eventuella extra eller onödiga kopior måste destrueras på säkert sätt. I förekommande fall måste originalhandlingar märkas med ”YTTERLIGARE KOPIERING INTE TILLÅTEN”. Kopiering måste utföras eller övervakas av betrodda personer. Eventuella extra eller onödiga kopior måste förstöras. Inga begränsningar.

Lagring av digital information Informationen ska lagras på fristående server i isolerat nät och inte på arbetsstationens lokala hårddisk. Servern ska vara placerad i ett godkänt låst serverrum I de fall då en server inte finns att tillgå ska informationen lagras på en krypterad separat hårddisk som när den inte används ska förvaras i ett säkerhetsskåp av klass SS 3492. Bärbar dator låses in, på motsvarande sätt, då den inte används. Åtkomst till information måste skyddas med stark autentisering. Informationen ska lagras på en fristående server i ett skyddat nät. Servern ska vara placerad i ett godkänt serverrum. Informationen får i undantagsfall lagras på en arbetsstation under förutsättning att hela lagringsmediet är krypterat och att IT-systemet inte delar ut resurser. Informationen får inte lagras i eller synkroniseras med en extern molntjänst. Informationen ska i första hand lagras på en fristående server och inte på arbetsstationens lokala hårddisk. Servern ska vara placerad i ett godkänt serverrum. Lagring i och synkronisering med molntjänster som tillhandahålls av KD är tillåten. Mobila medier Informationen får lagras på flyttbart lagringsmedium under förutsättning att hela mediet är krypterat samt att det hålls inlåst när det inte används. Dessa medier får inte lämnas utan uppsikt och inte heller flyttas utanför företagets lokaler såvida det inte skickas till annan behörig mottagare. Åtkomst till information måste skyddas med stark autentisering. Data måste krypteras. Mobila medieenheter, inklusive bärbara datorer, får inte lämnas obevakade och måste förvaras inlåsta när de inte används. Åtkomst till information måste skyddas med ett säkert lösenord. Mobila medieenheter, inklusive bärbara datorer, får inte lämnas obevakade och måste förvaras inlåsta när de inte används. Åtkomst till information måste skyddas med ett säkert lösenord. Muntliga samtal Muntliga samtal får endast ske där man kan försäkra sig om att det inte finns någon risk för att konversationer avlyssnas, antingen direkt eller med övervakningsteknik. Muntliga samtal får inte äga rum på en allmän plats eller där de kan avlyssnas. Muntliga samtal får inte äga rum där de kan avlyssnas. Post Information får endast skickas till auktoriserade mottagare. Informationen får inte sändas med internpost utan ska överlämnas personligen eller med bud. Vid försändning externt ska postbefordran med REK och mottagningsbevis alternativt bud användas. Information får endast skickas till auktoriserade mottagare. Leverans får ske med godkänt bud eller annan leveransmetod som kan spåras. Vid försändning med internpost ska dubbla förslutna kuvert

användas. Vid försändning externt ska postbefordran med REK och mottagningsbevis alternativt bud användas. Information får endast skickas till auktoriserade mottagare. Vid försändning med internpost ska förslutet kuvert användas. Extern posthantering får användas.
Publika nätverk, inklusive internet Direkta anslutningar från publika nätverk är inte tillåtna. Anslutningar måste göras via en DMZ implementerad med en säker brandvägg. Direkta anslutningar från publika nätverk är inte tillåtna. Anslutningar måste göras via en DMZ implementerad med en säker brandvägg. Anslutningar måste göras via en godkänd säker brandvägg. Regel om städat skrivbord Allt material måste låsas in när det inte används, till exempel i ett godkänt säkerhetsskåp. Allt material måste låsas in när det inte används. Allt material måste förvaras säkert när det inte används. Spårbarhet Varje inmatning (transaktion) eller förändring av information ska vara spårbar och riktigheten för varje inmatning eller förändring av informationen ska kunna verifieras. Informationen ska förses med ett högt skydd mot oavsiktlig eller avsiktlig förändring och får endast hanteras i ett skyddat nät med ett anpassat behörighetskontrollsystem. Informationen får inte lagras i eller synkroniseras med en molntjänst. Upphandlade tjänster som uppfyller kraven på verifiering av transaktioner är undantagna. Informationen ska vara spårbar och riktigheten ska kunna verifieras till exempel genom signering. Spårbarhet är inte nödvändig. Tele-, video- och webbkonferens Mottagarens identitet måste bekräftas och försiktighetsåtgärder vidtas för att förhindra avlyssning. Samtal får endast ske där man kan försäkra sig om att det inte finns någon risk för att det avlyssnas, antingen direkt eller med övervakningsteknik. Mottagarens identitet måste bekräftas och försiktighetsåtgärder vidtas för att förhindra avlyssning. Lämna inte meddelanden innehållande information av hög säkerhetsnivå på telefonsvarare eftersom de kan spelas upp av obehöriga personer, lagras på kommunala system eller lagras felaktigt till följd av felringning. Inga restriktioner.