Kammarkollegiet

Bilaga 3
Säkerhet

Innehåll

1 Allmänt

Denna bilaga beskriver övergripande den säkerhet som skall tillämpas för funktioner, produkter och tjänster i detta Ramavtal. Mer detaljerade säkerhetskrav kan definieras i leveransavtal vid avrop.

DGCs, och därmed även Kunds, informationstillgångar ska hanteras med god informationssäkerhet. DGCs informationstillgångar skall alltså skyddas mot alla typer av hot, både interna och externa, avsiktliga och oavsiktliga, fysiska och logiska, etc., på en passande nivå. Med god informationssäkerhet menar DGC att:

- Information som respektive medarbetare är beroende av för att kunna bedriva sina arbetsuppgifter är snabbt tillgänglig
- Informationen är tillförlitlig (riktighet)
- Information är endast tillgänglig för rätt instanser (sekretess)
- Information är spårbar i informationssystemen (spårbarhet)

Informationssäkerhetsarbetet ska bedrivas utifrån grunderna i ISO/IEC 27001 (ledningssystem för informationssäkerhet), ISO/IEC 27002 (riktlinjer för styrning av informationssäkerhet) samt Krisberedskapsmyndighetens Basnivå för Informationssäkerhet.

DGCs informationstillgångar och stödsystem är vitala för DGC och Kunds affärsverksamhet. För att säkerställa att IT-policy och riktlinjer för informationssäkerhet kontinuerligt håller en adekvat nivå och att dessa efterlevs krävs en disciplinerad organisation med en tydlig fördelning av ansvar samt ett systematiskt arbetssätt.

2 Säkerhet

DGCs säkerhetsarbete beskrivs i bolagets informationssäkerhetshandbok. Handboken består av en publik och en intern del. Den interna delen omfattar specifika riktlinjer och är ej publik. Fysisk säkerhet omfattas inte av informationssäkerhetshandboken. Detta regleras istället i interna rutiner eller avtal för samlokalisering på växelstation.

2.1 Administrativa säkerhetskrav

2.1.1 Basnivå för informationssäkerhet

Informationssäkerhetsarbetet på DGC utgår ifrån bolagets IT-policy. Hur informationssäkerhetsarbetet sedan regleras och styrs beskrivs i DGCs informations-säkerhetshandbok. Handboken omfattar beskrivning av Organisation och ansvarsfördelning samt Arbetsprocess för att beskriva informationssäkerhets-organisationens arbete, och vidare Riktlinjer samt Användar- och säkerhetspolicy för att vägleda verksamheten inom dessa frågor.

DGCs informationssäkerhetsarbete ligger väl i linje med relevanta delar ur Krisberedskapsmyndighetens rekommendation ” Basnivå för informationssäkerhet (BITS)” (KBM 2006:1). BITS har tillsammans med SS-ISO/IEC 27001:2006, Ledningssystem för informationssäkerhet – Krav, SS-ISO/IEC 27002:2005, Riktlinjer för styrning av informationssäkerhet, och PTS allmänna råd om god funktion och teknisk säkerhet samt uthållighet och tillgänglighet vid extraordinära händelser i fredstid efterlevs (PTSFS 2007:2) utgjort handledning för framtagning och löpande revision av Informationshandboken.

Fördelen DGC uppnår genom att arbeta med säkerhet enligt denna modell är en genomgående hög medvetenhet och kompetens hos personalen avseende säkerhetsfrågor. Dessutom kan processer och förebyggande åtgärder genomföras på bästa sätt i aktuellt verksamhetsområde. Vidare skapas centrala säkerhetsfunktioner för att vidareutveckla säkerhetsarbetet, följa marknaden, genomföra analyser, interna revisioner och efterlevnadskontroller.

Kammarkollegiets högt satta säkerhetskrav likväl som DGCs egna höga krav inom detta område kräver hög kompetens och erfarenhet samt strukturerat arbete och väl fungerande processer. Detta är något som DGC uppfyller med den säkerhetsorganisation som idag finns på plats. Organisationen ger en bra grund för att ta till sig ytterligare höjda krav med tiden, antingen genom att anpassa och utveckla DGCs policies och riktlinjer, eller genom att vid mer specifika kundanpassade krav hantera dessa uteslutande i kundprojekt.

2.1.2 Uppföljning och kontroll – säkerhetsrevision

Uppföljning av informationssäkerhetsarbetet är en förutsättning för att löpande säkerställa att skyddsnivån är anpassad till rådande hotbild och att organisationen efterlever riktlinjerna för informationssäkerhet i allmänhet. Dessutom har periodisk uppföljningen ett utbildningssyfte då utförandet sker i dialogform.

Nedan listas de huvudsakliga momenten inom uppföljning:

- Intern revision utförs fyra gånger per år tillsammans med Kvalitets- och Miljörevision
- Särskild säkerhetskontroll utförs då brister rapporterats från organisationen
- Löpande uppföljning av åtgärdsplan

Direkt efter genomförd kontroll delges den kontrollerade ett muntligt resultat. Kontrollen rapporteras därefter till ledningsgruppen för uppföljning inom respektive dotterbolag, där VD är ytterst ansvarig för att alla avvikelser hanteras. IT-chefen följer löpande upp åtgärdsplaner i dotterbolagen styrgrupper.

Revisionsplanen ses över 2 gånger per år i samförstånd mellan DGCs ledningsgrupp och IT-chef. Underlag för genomlysning av revisionsplan är resultat från löpande revisioner samt eventuella säkerhetsincidenter från perioden.

Samtliga DGCs rutiner är väl definierade och utarbetade efter mångåriga samarbeten med andra kunder. Dessa rutiner omfattar bland annat uppföljning och kontroll av avtalade servicenivåer. Eventuella avtalade säkerhetsnivåer som ligger utanför dessa ordinarie rutiner följs upp enligt kundunik samverkansplan.

2.1.3 Säkerhets- och sårbarhetsanalyser

DGC bedriver löpande säkerhets och sårbarhetsanalyser för att kartlägga hur hot mot vår infrastruktur kan motverkas eller avhjälpas med minsta möjliga påverkan för DGCs och därmed våra kunders verksamhet. Ett hot kan utgöras av en händelse som orsakar ett avbrott, intrångsrisk, eller dylikt som kan innebära ett hot mot tillgångar i DGCs infrastruktur.

Arbetet med säkerhets- och sårbarhetsanalys omfattar två delar. Dels kontinuitetsplanering, som syftar till att kartlägga risker, bedöma dessa och vidtaga eventuella förebyggande åtgärder, dels katastrofhantering, som syftar till att kartlägga risker, bedöma dessa och ta fram rutiner för att minimera inverkan om hotet skulle bli verklighet. Rutinerna för katastrofhantering omfattar även upprättande av katastrofledningsgrupp och deras ansvar och befogenheter vid en eventuell katastrof.

Genom DGCs rutiner för säkerhets- och sårbarhetsanalys minimeras risken för större avbrott eller andra hot mot säkerheten och konsekvenser av eventuella hot som de facto inträffar. Syftet med detta är att tillhandahålla en infrastruktur som är både tillförlitlig och säker.

DGC bistår Kund med konsultation och medverkan vid Kunds säkerhets- och sårbarhetsanalyser för berörda tjänster och funktioner.

2.1.4 Styrning och rutiner motsvarande SS-ISO/IEC 27002:2005

DGC tillämpar policys, processer, rutiner och strukturer avseende informationssäkerhet för leverans och produktion av erbjudna tjänster som väl motsvarar SS-ISO/IEC 27002:2005 i relevanta delar.

Informationssäkerhetsarbetet styrs ytterst av DGCs IT-policy och specificeras i DGCs informationssäkerhetshandbok, med undantag för fysisk och miljörelaterad säkerhet som regleras i separata riktlinjer, rutiner och avtal. Vidare ansvarar respektive verksamhetsområde för att följa dessa riktlinjer och själva upprätta processer, rutiner, checklistor och andra dokument som behövs för att säkerställa att verksamheten lever upp till policyn. Att handboken efterlevs regleras och kontrolleras sedan med utbildning och därpå följande revisioner.

2.1.5 Rutiner för drift och övervakning

Anbudsgivaren skall vid avrop presentera rutiner för drift och övervakning till beställaren.

DGCs avdelning för drift och underhåll består av tekniker som arbetar med daglig drift och underhåll av central infrastruktur samt tjänster inom Fasta operatörstjänster och Transmissionstjänster. Vissa tekniker utgör även del av Third Line Support inom DGC Helpdesk.

DGCs avdelning för drift och underhåll arbetar i enlighet med ITIL (Information Technology Infrastructure Library) med avseende på incidenter, rättningar och uppdateringar samt produktion.

Produktion handlar i första hand om utbyggnad av befintlig infrastruktur och konfiguration av logiska enheter i nätet. I de fall då det kan göras utan att påverka driften av den befintliga miljön görs det enligt rutin dagtid. Vid känsligare produktion planeras det till de servicefönster som finns avtalade med Kund.

Planerade rättningar och uppdateringar, såsom uppgraderingar av central infrastruktur, omläggningar och migreringar, genomförs under avtalade servicefönster. Akuta åtgärder görs enligt principen att minimera Avbrottstid och meddelas Kund så tidigt som möjligt.

För ytterligare information om DGCs övervakningssystem, se punkt 5.6 ”Övervakning” i Ramavtalets bilaga 4 ”Service och tillgänglighet”.

Övervakning av DGCs stamnät och Kunds tjänster görs centralt från DGC NOCs övervakningscentral i Stockholm. DGC NOC arbetar parallellt med DGC Helpdesk. Ansvarig för DGC NOC och övervakningen är driftchef för respektive område (Fasta operatörstjänster och Transmissionstjänster) och för Helpdesk ansvarar supportchef.

DGC har ett logiskt separerat övervakningsnät som är redundant kopplat till stamnätet. Övervakningen sker i första hand via ICMP och SNMP från ett antal övervakningsservrar. Servrar och applikationer är distribuerade logiskt och geografiskt i DGCs datahallar. Utöver aktiv övervakning hanteras även larm för störningar i kommunikation och tjänst, vilka kommer in via SYSLOG. Samtliga händelser som ankommer behandlas av övervakningsservrar, loggas, processas och presenteras via olika gränssnitt för DGC NOC.

Övervakningen hanterar bland annat länkstatus, belastning av hårdvara och länkar, paketförluster, svarstider och händelser (av hårdvara identifierade larm). Övervakning sker dygnet runt, alla dagar.

DGC Helpdesk larmas av DGC NOC vid central driftstörning och påbörjar då felavhjälpning. Vid larm för enskild kundanslutning krävs först Kunds felanmälan för påbörjad felavhjälpning om inte annat avtalas i leveransavtalet.

Kund ges tillgång till spegling av DGCs övervakning enligt punkt 3.10.2 ”Spegling av övervakning” i Ramavtalets bilaga 2 ”Funktioner, produkter, tjänster och priser”.

DGC presenterar detaljerade rutiner för drift och övervakning för Kund vid avrop.

2.2 Allmänna tekniska säkerhetskrav

2.2.1 Fysisk infrastruktur

Leverantören skall till Kund tydligt kunna redogöra för den nationella fysiska infrastruktur och det egna kommunikationsnät som tjänsten är baserad på med fysisk placering av relevanta noder och nationella framföringsvägar för fysiskt media.

DGCs fysiska infrastruktur är i huvudsak placerad i lokaler för så kallad samlokalisering hos Skanova. Utöver detta har DGC även infrastruktur i ett antal datahallar och andra lokaler. För tillgång till Skanovas lokaler krävs certifiering och personliga passerkort med koder. Tillträdet övervakas och administreras av Skanova. Övriga datahallar och utrymmen kräver behörighet med kort, koder och nycklar för tillträde.

DGCs transmissionstjänster bygger på MPLS-teknologi (Multiprotocol Label Switching) för att erbjuda de säkraste och mest stabila privata nätverken. Med MPLS transporteras all trafik igenom DGCs stamnät vilket möjliggör hög kapacitet och automatisk omkoppling vid eventuella driftstörningar. DGCs stamnät är byggt i nationella och lokala ringstrukturer med redundant hårdvara för högsta möjliga driftsäkerhet.

DGCs nätstrategi är att äga de delar av nätinfrastrukturen som säkerställer att DGC kan erbjuda sina slutkunder attraktiva tjänster till konkurrenskraftiga priser. DGC har därför etablerat egen utrustning i hittills cirka 270 av TeliaSoneras telestationer, från Kiruna i norr till Ystad i söder, för att kunna ansluta merparten av den svenska företagsmarknaden och offentlig sektor i ett eget nät. DGC hyr också stamnäts- och stadsnätsförbindelser av nätägare för att koppla samman denna utrustning i telestationerna till ett eget rikstäckande nät, designat i ovan nämnda ringstrukturer för högsta möjliga tillgänglighet.

DGC använder ett tjugotal underleverantörer för att knyta samman alla delar av sitt nät, men den överlägset största underleverantören är TeliaSonera. Tjänsterna som DGC hyr av TeliaSonera är reglerade tjänster, som i huvudsak levereras av TeliaSoneras nätbolag Skanova Access och övriga tjänster som levereras av TeliaSoneras nätoperatör International Carrier.

Vid avrop lämnar DGC ytterligare information om den fysiska infrastrukturen vid begäran. DGC kan komma att begära att denna information skall omfattas av sekretess. Anledning till detta är att viss information kan utgöra företagshemligheter.

Kund ansvarar för skalskydd avseende all kundplacerad hårdvara.

2.2.2 Uthållighet

DGC tillämpar policys, processer, rutiner och strukturer avseende informationssäkerhet för leverans och produktion av erbjudna tjänster som väl motsvarar PTS allmänna råd om god funktion och teknisk säkerhet samt uthållighet och tillgänglighet vid extraordinära händelser i fredstid efterlevs (PTSFS 2007:2).

Kontinuerligt och systematiskt säkerhetsarbete bedrivs löpande. Detta omfattar riskanalys såväl som riskhantering. Genom löpande säkerhets och sårbarhetsanalyser kartläggs hur hot mot vår infrastruktur kan motverkas eller avhjälpas med minsta möjliga påverkan för DGCs och därmed våra kunders verksamhet. Ett hot kan utgöras av en händelse som orsakar ett avbrott, intrångsrisk, eller dylikt som kan innebära ett hot mot tillgångar i DGCs infrastruktur.

Arbetet omfattar två delar. Dels kontinuitetsplanering, som syftar till att kartlägga risker, bedöma dessa och vidtaga eventuella förebyggande åtgärder, dels katastrofhantering, som syftar till att kartlägga risker, bedöma dessa och ta fram rutiner för att minimera inverkan om hotet skulle bli verklighet. Rutinerna för katastrofhantering omfattar även upprättande av katastrofledningsgrupp och deras ansvar och befogenheter vid en eventuell katastrof.

Genom DGCs rutiner för säkerhets- och sårbarhetsanalys minimeras risken för större avbrott eller andra hot mot säkerheten och konsekvenser av eventuella hot som de facto inträffar. Syftet med detta är att tillhandahålla en infrastruktur som är både tillförlitlig och säker.

2.2.3 Skydd av tjänst

Beskriv hur tjänster skyddas mot otillbörligt nyttjande, intrång, avlyssning, annan manipulering, sabotage och sammankoppling med andra kunders kommunikationstjänster och hur spårbarhet av förändringar och händelser i tjänsten kan säkerställas.

DGCs, och därmed även Kunds, informationstillgångar skall hanteras med god informationssäkerhet. DGCs informationstillgångar skall alltså skyddas mot alla typer av hot, både interna och externa, avsiktliga och oavsiktliga, fysiska och logiska, etc., på en passande nivå. Med god informationssäkerhet menar DGC att:

- Information som respektive medarbetare är beroende av för att kunna bedriva sina arbetsuppgifter är snabbt tillgänglig
- Informationen är tillförlitlig (riktighet)
- Information är endast tillgänglig för rätt instanser (sekretess)
- Information är spårbar i informationssystemen (spårbarhet)

Informationssäkerhetsarbetet ska bedrivas utifrån grunderna i ISO/IEC 27001 (ledningssystem för informationssäkerhet), ISO/IEC 27002 (riktlinjer för styrning av informationssäkerhet) samt Krisberedskapsmyndighetens Basnivå för Informationssäkerhet.

DGCs IT-chef utvärderar löpande om organisationen efterlever DGCs IT-policy.

Tjänster inom Fasta operatörstjänster och Transmissionstjänster skyddas i två nivåer. Dels i form av skalskydd där den fysiska infrastrukturen skyddas med ett begränsat och kontrollerat tillträde. Vidare skyddas tjänsterna logiskt med autentiseringssystem i all central infrastruktur. För åtkomst krävs säkra anslutningar, användarnamn och lösenord vilka administreras centralt. Systemen för autentisering är baserade på branschpraxis och använder sig av bland annat tacacs och ssh.

Den logiska säkerheten i näten baseras på Ethernet MPLS-teknik, vilket är en standard för att ge anslutningar unika identifieringar, vilket i sin tur gör att två kunders transmissionstjänster inte förväxlas. DGC allokerar ett unikt MPLS-id till varje anslutning och binder ihop dessa till kundunika VPN (så kallade BGP/MPLS-VPN).

Detta säkerställer sekretess och informationens riktighet.

Alla förändringar i DGCs infrastruktur loggas för att möjliggöra uppföljning och efterkontroll. Åtkomst till DGCs utrustning och maskiner i växelstationer görs ifrån ett separerat underhållsnät. Accesskontroll-servrar och versionshanteringssystem kontrollerar och för logg över de förändringar som utförs i nätet. Detta säkerställer informationens spårbarhet.

Kund ansvarar för skalskydd avseende all kundplacerad hårdvara.

2.2.4 Rapportering

Anbudsgivaren skall omedelbart rapportera brister i skyddet av eller angrepp mot tjänsten eller till tjänsten relaterad infrastruktur till Kund.

DGC rapporterar omedelbart brister i skyddet av eller angrepp mot tjänsten eller till tjänsten relaterad infrastruktur till Kund. Kund ansvarar för att förse DGC med kontaktperson eller kontaktyta för detta i enlighet med leveransavtalet eller kundunik samverkansplan.

DGCs informationssäkerhetshandbok klassificerar säkerhetsincidenter och definierar DGCs interna rapporteringsrutin för dessa.

DGCs tjänster inom Fasta operatörstjänster och Transmissionstjänster kan missbrukas för att exempelvis sprida barnporr eller hatpropaganda, sälja narkotika eller skicka oönskad reklam (spam). DGC skall inte på något sätt medverka till sådana aktiviteter och skall alltid polisanmäla misstänkta lagöverträdelser inom detta område.

Börspåverkande information får inte distribueras endast till Kund utan skall offentliggöras så att den snabbt och på ett icke diskriminerande sätt blir tillgänglig för allmänheten.