Uttalande om Tillämplighet

Statement of Applicability

ISO 27001

Säkerhetsåtgärd	Beskrivning	Relevant	Referens/ motivering	Definition
5.1.1 Informationssäkerhetspolicy	Ett regelverk för informationssäkerhet, som inkluderar informationssäkerhetspolicyn, bör fastställas, godkännas av ledningen, publiceras och kommuniceras till medarbetare och relevanta externa parter.	Ja	Omvärldsanalys - Rättsliga krav	Informationssäkerhet och rutinbeskrivning för LIS Serverhallen, instruktioner för personal, Affärsverkens IT-säkerhetsinstruktion, Informationssäkerhetspolicy för Affärsverkens serverhall. Förhållningsregler för Serverhallen, Riskanteringsprocess.
5.1.2 Granskning av regelverk för informationssäkerhet	Regelverket (inklusive informationssäkerhetspolicyn) för informationssäkerhet bör granskas med planerade intervall, eller om betydande förändringar sker, för att säkerställa deras fortsatta lämplighet, riktighet och verkan.	Ja	Verksamhetsanalys	Ledningens genomgång, interna revisioner och revidering av riskbedömning.
6.1.1 Informationssäkerhetsroller och ansvar	Allt ansvar för informationssäkerhet bör definieras och tilldelas.	Ja	Verksamhetsanalys	Rutinbeskrivning för LIS Serverhallen med beskrivna roller. Tydligt ägarskap och ansvar för riskerna skall finnas i riskbedömningen.
6.1.2 Uppdelning av arbetsuppgifter	Ansvar och ansvarsområden som står i konflikt med varandra bör åtskiljas för att minska möjligheterna för obehörig eller oavsiktlig ändring eller missbruk av organisationens tillgångar.	Ja	Verksamhetsanalys	Organisatorisk särskiljning på Säkerhetsansvarig och IT organisation.
6.1.3 Kontakt med myndigheter	Lämpliga kontakter med relevanta myndigheter bör upprätthållas.	Ja	Omvärldsanalys - Rättsliga krav	Affärsverkens rapporteringsskyldighet till ägare och myndigheter vid incidenter.
6.1.4 Kontakt med särskilda intressegrupper	Lämpliga kontakter med särskilda intressegrupper eller andra forum för säkerhetsspecialister och branschorganisationer bör upprätthållas.	Ja	Omvärldsanalys	Systematisk omvärldsbevakning och dialog med intressenter både intern och externa genomförs löpande.

6.1.5 Informationssäkerhet i projektledning	Informationssäkerhet bör hanteras inom projektledning, oavsett typ av projekt.	Ja	Verksamhetsanalys	Affärsverkens projektledningsmodell innefattar informationssäkerhetsmål. Bedömning av informationssäkerhetsrisker bedöms vid riskhanteringen och informationssäkerhet kommer att ingå i alla faser av projektmetodiken.
6.2.1 Regler för mobila enheter	Regler och stödjande säkerhetsåtgärder bör antas för att hantera de risker som användning av mobila enheter medför.	Ja	Riskanalys	Affärsverkens IT-säkerhetsinstruktion.
6.2.2 Distansarbete	Regler och stödjande säkerhetsåtgärder bör införas för att skydda information som nås, bearbetas eller lagras på distansarbetsplatser.	Ja	Riskanalys	Affärsverkens IT-säkerhetsinstruktion, arbete utanför affärsverkens lokaler.
7.1.1 Bakgrundskontroll	Bakgrundskontroll på alla sökande för anställning bör utföras i enlighet med relevanta författningar och etiska krav och bör stå i proportion till verksamhetskraven, klassificeringen av information som de ges behörighet till och de upplevda riskerna.	Ja	Verksamhetsanalys	Policy vid rekrytering av nya medarbetare.
7.1.2 Anställningsvillkor	Avtal med anställda och leverantörer bör ange deras och organisationens ansvar för informationssäkerhet.	Ja	Verksamhetsanalys	Affärsverkens IT-säkerhetsinstruktion, anställningsavtal med anställda, Personuppgiftspolicy för anställda.
7.2.1 Ledningens ansvar	Ledningen bör kräva att alla anställda och leverantörer tillämpar informationssäkerhetskrav i enlighet med för organisationen fastställda regler och rutiner.	Ja	Verksamhetsanalys	Sekretessavtal samt Affärsverkens IT-säkerhetsinstruktion.
7.2.2 Medvetenhet, utbildning och fortbildning vad gäller informationssäkerhet	Alla organisationens anställda och, i förekommande fall, leverantörer ska erhålla lämplig utbildning och fortbildning för ökad medvetenhet, samt regelbundna uppdateringar vad gäller organisationens policy, regelverk och rutiner i den omfattning som är relevant för deras befattning.	Ja	Verksamhetsanalys	Rutinbeskrivningen för LIS Serverhallen.
7.2.3 Disciplinär process	Det ska finnas en formell och kommunicerad disciplinär process för att vidta åtgärder mot anställda som har brutit mot gällande informationssäkerhetsregler.	Ja	Verksamhetsanalys	Affärsverkens IT-säkerhetsinstruktion, Informationssäkerhetspolicy för Serverhallen, samt användaravtal.

7.3.1 Avslut eller ändring av anställds ansvar	Ansvar för informationssäkerhet och skyldigheter som förblir gällande efter avslut eller ändring av anställning ska definieras och kommuniceras till den anställde eller leverantören samt verkställas.	Ja	Verksamhetsanalys	Användaravtal, leverantörsavtal.
8.1.1 Inventering av tillgångar	Tillgångar som är relaterade till information och informationsbehandlingsresurser ska identifieras och en förteckning över dessa tillgångar ska upprättas och underhållas.	Ja	Verksamhetsanalys	Verksamhetsanalys för serverhallen, Karta över informationstillgångar för serverhallen och Affärsverkens Roller och Systemansvar.
8.1.2 Ägarskap av tillgångar	Tillgångar som återfinns i sammanställningen ska tilldelas ägare.	Ja	Verksamhetsanalys	Verksamhetsanalys för serverhallen och Affärsverkens Roller och Systemansvar.
8.1.3 Tillåten användning av tillgångar	Regler för tillåten användning av information, och tillgångar som är relaterade till information och informationsbehandlingsresurser, ska identifieras, dokumenteras och införas.	Ja	Verksamhetsanalys	Affärsverken IT-Säkerhetsinstruktion, verksamhetsanalys serverhallen.
8.1.4 Återlämnande av tillgångar	Alla anställda och externa användare ska återlämna alla organisationens tillgångar som de förfogar över då deras anställning, uppdrag eller avtal upphör.	Ja	Verksamhetsanalys	Checklista för Upphörande av anställning, samt Upphörande av anställning eller pensionering för avregistrering i systemen.
8.2.1 Klassning av information	Information ska klassas i termer av rättsliga krav, värde, verksamhetsbetydelse och känslighet för obehörigt röjande eller modifiering.	Ja	Riskanalys	Verksamhetsanalys för serverhallen.
8.2.2 Märkning av information	En lämplig uppsättning rutiner för märkning av information ska utvecklas och införas i enlighet med den modell för informationsklassning som antagits av organisationen.	Ja	Riskanalys	Rutinbeskrivning för märkning av information.
8.2.3 Hantering av tillgångar	Rutiner för hantering av tillgångar ska utvecklas och införas i enlighet med modell för informationsklassning som antagits av organisationen	Ja	Verksamhetsanalys	Rutinbeskrivning för LIS Serverhallen samt i verksamhetsanalys för serverhallen.
8.3.1 Hantering av flyttbara lagringsmedia	Rutiner ska införas för hantering av flyttbara lagringsmedia i enlighet med modell för informationsklassning som antagits av organisationen.	Ja	Riskanalys	Affärsverken IT-säkerhetsinstruktion.

8.3.2 Avveckling av lagringsmedia	Lagringsmedia ska avvecklas på ett säkert sätt när det inte längre behövs med stöd av formella rutiner.	Ja	Riskanalys	Affärsverken IT-säkerhetsinstruktion.
8.3.3 Transport av fysiska lagringsmedia	Lagringsmedia som innehåller information ska skyddas mot obehörig åtkomst, missbruk eller förvanskning under transport.	Ja	Riskanalys	Affärsverken IT-säkerhetsinstruktion.
9.1.1 Regler för styrning av åtkomst	Regler för styrning av åtkomst ska upprättas, dokumenteras och vara föremål för uppföljning utifrån verksamhets- och informationssäkerhetskrav.	Ja	Riskanalys	Auktorisationsprocess IT. Affärsverken IT-säkerhetsinstruktion.
9.1.2 Tillgång till nätverk och nätverkstjänster	Användare ska endast ges tillgång till nätverk och nätverkstjänster som de specifikt beviljats tillstånd för.	Ja	Riskanalys	Se 9.1.1
9.2.1 Registrering och avregistrering av användare	En formell process för registrering och avregistrering av användare ska införas för att möjliggöra tilldelning av åtkomsträttigheter.	Ja	Riskanalys	Auktorisationsprocess IT.
9.2.2 Tilldelning av användaråtkomst	En formell process för tilldelning av användaråtkomst ska införas för tilldelning och återkallande av åtkomsträttigheter för alla typer av användare till alla system och tjänster.	Ja	Riskanalys	Se 9.1.1
9.2.3 Hantering av privilegierade åtkomsträttigheter	Tilldelning och användning av privilegierade åtkomsträttigheter ska begränsas och styras.	Ja	Riskanalys	Se 9.1.1
9.2.4 Hantering av användares konfidentiella autentiseringsinformation	Tilldelningen av konfidentiell autentiseringsinformation ska styras genom en formell hanteringsprocess.	Ja	Riskanalys	Se 9.1.1, Intern-IT rutiner
9.2.5 Granskning av användares åtkomsträttigheter	Ägare av tillgångar ska med jämna mellanrum granska användarnas åtkomsträttigheter.	Ja	Riskanalys	Systemspecifika rutiner för granskning av åtkomsträttigheter.
9.2.6 Borttagning eller justering av åtkomsträttigheter	Åtkomsträttigheterna för alla anställda, och externa användare, till information och informationsbehandlingsresurser ska tas bort vid avslutande av deras anställning, avtal eller uppdrag eller justeras vid förändringar.	Ja	Riskanalys	Auktorisationsprocess IT.
9.3.1 Användning av konfidentiell autentiseringsinformation	Användare ska åläggas att följa organisationens arbetssätt vid användning av konfidentiell autentiseringsinformation.	Ja	Verksamhetsanalys	Lösenordskrav AD och Affärsverken IT-säkerhetsinstruktion.

9.4.1 Begränsning av åtkomst till information	Tillgång till information och systemfunktioner ska begränsas i enlighet med regler för styrning av åtkomst.	Ja	Riskanalys	Lösenordskrav AD och Affärsverken IT-säkerhetsinstruktion, gällande systemspecifika riktlinjer och AD.
9.4.2 Säkra inloggningsrutiner	Där regler för styrning av åtkomst så kräver, ska tillgång till system och tillämpningar styras genom säkra inloggningsrutiner.	Ja	Riskanalys	Lösenordskrav AD och Affärsverken IT-säkerhetsinstruktion, gällande systemspecifika riktlinjer och AD.
9.4.3 System för lösenordshantering	System för lösenordshantering ska vara interaktiva och ska säkerställa kvalitativa lösenord.	Ja	Riskanalys	Lösenordskrav AD och Affärsverken IT-säkerhetsinstruktion, gällande systemspecifika riktlinjer och AD.
9.4.4 Användning av privilegierade verktygsprogram	Användning av verktygsprogram som kan ha förmåga att kringgå säkerhetsåtgärder i system och tillämpningar ska begränsas och styras strikt.	Nej	Verksamhetsanalys	Förekommer ej.
9.4.5 Åtkomstkontroll till källkod för program	Tillgången till källkod för program ska begränsas.	Nej	Verksamhetsanalys	Förekommer ej
10.1.1 Regler för användning av kryptografiska säkerhetsåtgärder	Regler för användning av kryptografiska säkerhetsåtgärder för skydd av information ska utvecklas och införas.	Ja	Verksamhetsanalys	Affärsverken IT-säkerhetsinstruktion.
10.1.2 Nyckelhantering	Regler för användning, skydd och giltighetstid för kryptografiska nycklar för deras hela livscykel ska utvecklas och införas.	Ja	Riskanalys	Administration av berörda system (Intern-IT)
11.1.1 Fysiska säkerhetsavgränsningar	Fysiska avgränsningar ska definieras och användas för att skydda områden som innehåller antingen känslig eller kritisk information och informationsbehandlingsresurser.	Ja	Riskanalys	Riskbedömning
11.1.2 Fysiska tillträdesbegränsningar	Säkra områden ska skyddas genom lämpliga säkerhetsåtgärder för att säkerställa att endast behörig personal får tillträde.	Ja	Riskanalys	Riskbedömning
11.1.3 Säkerställande av kontor, rum och anläggningar	Fysisk säkerhet för kontor, rum och anläggningar ska utformas och tillämpas.	Ja	Riskanalys	Riskbedömning
11.1.4 Skydd mot yttre och miljörelaterade hot	Fysiskt skydd mot naturkatastrofer, illvilliga angrepp eller olyckor ska utformas och införas.	Ja	Riskanalys	Riskbedömning
11.1.5 Arbeta i säkra utrymmen	Rutiner för att arbeta i säkra utrymmen ska utformas och tillämpas.	Ja	Riskanalys	Förhållningsregler samt instruktioner.
11.1.6 Leverans- och lastningsområden	Åtkomstpunkter såsom leverans- och lastningsområden och andra punkter där obehöriga personer kan komma in i lokalerna ska styras och om möjligt isoleras från informationsbehandlingsresurser för att undvika obehörig åtkomst.	Nej	Verksamhetsanalys	Ingen leverans sker i angränsning till serverhallen.
11.2.1 Placering och skydd av utrustning	Utrustning ska placeras och skyddas för att minska riskerna för	Ja	Riskanalys	Säkerhetsåtgärder enligt riskbedömning avseende utformning och design.

	miljörelaterade hot och faror och möjligheter för obehörig åtkoms			
11.2.2 Tekniska försörjningssystem	Utrustning ska skyddas från elavbrott och andra störningar som orsakas av fel i tekniska försörjningssystem.	Ja	Riskanalys	Redundans och reservkraft.
11.2.3 Kablagesäkerhet	Kablage för ström och telekommunikation för data eller stödjande informationstjänster ska skyddas från avlyssning, störningar och skada.	Ja	Riskanalys	Regler för kabeldragning i kundavtal.
11.2.4 Underhåll av utrustning	Utrustning ska underhållas korrekt för att säkerställa fortsatt tillgänglighet och riktighet.	Ja	Riskanalys	Service- och underhållsschema.
11.2.5 Utförsel av tillgångar	Utrustning, information eller program ska inte avlägsnas utanför organisationens lokaler utan tillstånd.	Ja	Verksamhetsanalys	Rutiner för hantering av utrustning, Affärsverkens IT-Säkerhetsinstruktion.
11.2.6 Säkerhet för utrustning och tillgångar utanför organisationens lokaler	Säkerhet ska tillämpas på tillgångar utanför organisationens lokaler med hänsyn tagen till de särskilda risker som är förknippade med att arbeta utanför organisationens lokaler.	Ja	Riskanalys	Kravställning och regler för hantering utanför organisationens lokaler, Affärsverken IT-säkerhetsinstruktion.
11.2.7 Säker kassering eller återanvändning av utrustning	All utrustning som innehåller lagringsmedia ska granskas för att säkerställa att all känsliga data och licensierade program har avlägsnats eller säkert överskrivits före kassering eller återanvändning.	Ja	Riskanalys	Affärsverken IT-säkerhetsinstruktion
11.2.8 Obevakad utrustning som hanteras av användare	Användare ska säkerställa att obevakad utrustning har lämpligt skydd.	Ja	Verksamhetsanalys	Affärsverkens IT-säkerhetsinstruktion.
11.2.9 Regel om rent skrivbord och tom skärm	En regel ska antas för rent skrivbord med avseende på papper och flyttbara lagringsmedia och en regel för tom skärm på informationsbehandlingsresurser ska antas.	Ja	Omvärldsanalys - Rättsliga krav	Affärsverken IT-säkerhetsinstruktion.
12.1.1 Dokumenterade driftsrutiner	Driftsrutiner ska dokumenteras och göras tillgängliga för alla användare som behöver dem.	Ja	Annat skäl	Process incidenthantering vid driftlarm.
12.1.2 Ändringshantering	Förändringar i organisationen, verksamhetsprocesser eller informationsbehandlingsresurser och system som påverkar informationssäkerheten ska styras.	Ja	Annat skäl	Rutiner för ändringshantering.
12.1.3 Kapacitetshantering	Användningen av resurser ska övervakas samt justeras och prognoser av framtida kapacitetskrav ska göras för att säkerställa nödvändig systemprestanda.	Ja	Verksamhetsanalys	Rutiner för övervakning av systemresurser och prestanda.

12.1.4 Separation av utvecklings-, test och driftmiljöer	Utvecklings-, test- och driftmiljöer ska vara separerade för att minska risken för obehörig åtkomst eller ändringar i driftmiljön.	Ja	Verksamhetsanalys	Systemspecifika åtgärder.
12.2.1 Säkerhetsåtgärder mot skadlig kod	Upptäckande, förebyggande och återställande säkerhetsåtgärder för att skydda mot skadlig kod ska införas i kombination med säkerställande av en lämplig nivå av medvetenhet hos användarna.	Ja	Verksamhetsanalys	Antivirusprogram.
12.3.1 Säkerhetskopiering av information	Säkerhetskopior av information, program och speglingar av system ska tas och testas regelbundet i enlighet med överenskomna regler för säkerhetskopiering.	Ja	Verksamhetsanalys	Systemspecifika regler och rutiner för säkerhetskopiering.
12.4.1 Loggning av händelser	Händelseloggar som registrerar användaraktiviteter, avvikelser, fel och informationssäkerhetshändelser bör skapas, bevaras och granskas regelbundet	Ja	Verksamhetsanalys	Hantering i respektive system.
12.4.2 Skydd av logginformation	Loggningsverktyg och logginformation bör skyddas mot manipulation och obehörig åtkomst	Ja	Verksamhetsanalys	Hantering i respektive system.
12.4.3 Administratörs- och operatörsloggar	Systemadministratörers och systemoperatörers aktiviteter bör loggas och loggarna bör skyddas och granskas regelbundet	Ja	Verksamhetsanalys	Hantering i respektive system., rutiner för loggning och granskning.
12.4.4 Synkronisering av tid	Systemklockorna i alla relevanta informationsbehandlingssystem inom en organisation eller säkerhetsdomän bör synkroniseras mot en och samma referenskälla för tid	Ja	Verksamhetsanalys	Systemspecifika åtgärder.
12.5.1 Installation av program på driftssystem	Rutiner bör införas för att styra installation av program på driftsystem	Ja	Verksamhetsanalys	Rutiner för styrning av installationer, enligt ändringsprocess.
12.6.1 Hantering av tekniska sårbarheter	Information om tekniska sårbarheter i de informationssystem som används bör erhållas i tid, organisationens exponering för sådana sårbarheter analyseras och lämpliga åtgärder vidtas för att behandla den tillhörande risken	Ja	Verksamhetsanalys	Affärsverkens IT-Säkerhetsinstruktion. Rutiner för patch rutiner och uppgraderingar.
12.6.2 Restriktioner för installation av program	Regler för programinstallationer som utförs av användare bör upprättas och införas	Ja	Verksamhetsanalys	Affärsverkens IT-säkerhetsinstruktion, Riktlinjer systemförvaltning.
12.7.1 Revisionskontroll av informationssystem	Revisionskrav och revisionsaktiviteter som omfattar verifiering av status på driftsystem bör planeras noggrant och godkännas för att minimera störningar i verksamhetsprocesser	Ja	Annat skäl	Riktlinjer systemförvaltning.
13.1.1 Säkerhetsåtgärder för nätverk	Nätverk bör hanteras och styras för att skydda information i system och tillämpningar	Ja	Verksamhetsanalys	Affärsverken IT-Säkerhetsinstruktion.

13.1.2 Säkerhet hos nätverkstjänster	Säkerhetsmekanismer, tjänstenivåer och ledningskrav vad gäller alla nätverkstjänster bör identifieras och inkluderas i avtal för nätverkstjänster, oavsett om dessa tjänster tillhandahålls internt eller som outsourcade tjänster	Ja	Verksamhetsanalys	Affärsverken IT-Säkerhetsinstruktion.
13.1.3 Separation av nätverk	Grupper av informationstjänster, användare och informationssystem bör separeras i nätverk	Ja	Verksamhetsanalys	Affärsverken IT-Säkerhetsinstruktion.
13.2.1 Regler och rutiner för informationsöverföring	Formella regler, rutiner och säkerhetsåtgärder bör vara införda för att skydda överföring av information genom användning av alla typer av kommunikationsmedel	Ja	Verksamhetsanalys	Informationsklassning, kommunikationsplan.
13.2.2. Överenskommelser om informationsöverföring	Säker överföring av verksamhetsinformation mellan organisationen och externa parter bör vara reglerad i överenskommelser	Ja	Verksamhetsanalys	Avtal och instruktioner med leverantörer.
13.2.3 Elektronisk meddelandehantering	Information som hanteras genom elektronisk meddelandehantering bör ha tillräckligt skydd	Ja	Verksamhetsanalys	Affärsverken IT-Säkerhetsinstruktion.
13.2.4 Konfidentialitet och förbindelser om konfidentialitet	Krav på konfidentialitet eller förbindelser rörande konfidentialitet som återspeglar organisationens behov av skydd av information bör identifieras, regelbundet granskas och dokumenteras	Ja	Verksamhetsanalys	Systematisk riskbedömning och kontroll inom LIS för serverhallen.
14.1.1 Analys och specifikation av informationssäkerhetskrav	Krav som rör informationssäkerhet bör inkluderas i kraven för nya informationssystem eller förbättringar av befintliga informationssystem	Ja	Verksamhetsanalys	Roller och Systemansvar.
14.1.2 Säkerställande av programtjänster på publika nätverk	Information i programtjänster på publika nätverk bör skyddas från bedräglig aktivitet, avtalstvist och obehörigt röjande och modifiering	Ja	Verksamhetsanalys	Riktlinjer i Affärsverken IT-Säkerhetsinstruktion.
14.1.3 Skydd av transaktioner i tillämpningstjänster	Information hanterad som del i programtjänsters transaktioner bör skyddas för att förhindra ofullständig överföring, felaktig styrning av nätverkstrafik, obehörig ändring av meddelanden, obehörigt röjande, obehörig duplicering av meddelanden eller åter uppspelning	Ja	Verksamhetsanalys	Affärsverken har idag nätverk segmentering, samt VPN anslutning.
14.2.1 Regler för säker utveckling	Regler för utveckling av program och system bör upprättas och tillämpas vid systemutveckling inom organisationen	Nej	Välj	Ingen mjukvaruutveckling sker inom företaget eller LIS för Serverhallen.
14.2.2 Rutiner för hantering av systemförändringar	Systemförändringar inom utvecklingscykeln bör styras genom användning av formella riktlinjer för ändringshantering	Nej	Välj	Ingen mjukvaruutveckling sker inom företaget eller LIS för Serverhallen.
14.2.3 Tekniska granskningar av tillämpningar efter ändringar i driftsmiljö	Systemförändringar inom utvecklingscykeln bör styras genom användning av formella riktlinjer för ändringshantering	Nej	Välj	Ingen mjukvaruutveckling sker inom företaget eller LIS för Serverhallen.

14.2.4 Restriktioner för ändringar av programpaket	Ändringar av programpaket bör förhindras eller begränsas till nödvändiga ändringar och alla ändringar bör styras noggrant	Nej	Välj	Ingen mjukvaruutveckling sker inom företaget eller LIS för Serverhallen.
14.2.5 Principer för utveckling av säkra system	Riktlinjer för utveckling av säkra system bör upprättas, dokumenteras, underhållas och tillämpas vid alla införanden av informationssystem	Nej	Välj	Ingen mjukvaruutveckling sker inom företaget eller LIS för Serverhallen.
14.2.6 Säker utvecklingsmiljö	För systemutvecklings- och integrationsåtgärder bör organisationen upprätta och på lämpligt sätt skydda säkra utvecklingsmiljöer som sträcker sig över systemets hela livscykel	Nej	Välj	Ingen mjukvaruutveckling sker inom företaget eller LIS för Serverhallen.
14.2.7 Outsourcad utveckling	Organisationen bör övervaka och styra outsourcad systemutveckling	Nej	Välj	Ingen mjukvaruutveckling sker inom företaget eller LIS för Serverhallen.
14.2.8 Säkerhetstestning	Säkerhetsfunktionalitet bör testas vid utveckling	Nej	Välj	Ingen mjukvaruutveckling sker inom företaget eller LIS för Serverhallen.
14.2.9 Acceptanstestning av system	Program för acceptanstester och relaterade kriterier bör fastställas för nya informationssystem, uppgraderingar och nya versioner	Nej	Välj	Ingen mjukvaruutveckling sker inom företaget eller LIS för Serverhallen.
14.3.1 Skydd av testdata	Testdata bör noggrant väljas ut, skyddas och styras	Nej	Välj	Ingen mjukvaruutveckling sker inom företaget eller LIS för Serverhallen.
15.1.1 Informationssäkerhetsregler för leverantörsrelationer	Informationssäkerhetskrav för att reducera riskerna förknippade med leverantörers åtkomst till organisationens tillgångar bör avtalas med leverantören och dokumenteras	Ja	Verksamhetsanalys	Krav på leverantörer i leverantörsavtal och bilagor.
15.1.2 Hantering av säkerhet inom leverantörsavtal	Alla relevanta informationssäkerhetskrav bör upprättas och avtalas med varje leverantör som kan tillgå, behandla, lagra, kommunicera eller som tillhandahåller infrastrukturkomponenter för organisationens information	Ja	Verksamhetsanalys	Krav på leverantörer finns i leverantörsavtal och bilagor.
15.1.3 Försörjningskedja för informations- och kommunikationsteknologi	Avtal med leverantörer bör innehålla krav på att hantera informationssäkerhetsriskerna förknippade med försörjningskedjan för tjänster och produkter baserade på informations- och kommunikationsteknologi	Ja	Verksamhetsanalys	Krav på leverantörer finns i leverantörsavtal och bilagor.
15.2.1 Övervakning och granskning av leverantörstjänster	Organisationer bör regelbundet övervaka, granska och revidera leverantörers tjänsteleverans	Ja	Verksamhetsanalys	Leverantörsbedömningar genomförs regelbundet.
15.2.2 Ändringshantering av leverantörers tjänster	Ändringar av tillhandahållande av tjänster från leverantörer, inklusive underhåll och förbättring av befintlig informationssäkerhetspolicy med tillhörande regelverk och befintliga rutiner bör hanteras, med beaktande av informationens, systemens och processernas kritiska betydelse för verksamheten och riskerna ska omvärderas	Ja	Verksamhetsanalys	Systematisk kommunikation och dialog, Rutinbeskrivning för LIS för Serverhallen.

16.1.1 Ansvar och rutiner	Ledningsansvar och rutiner bör fastställas för att säkerställa snabb, verkningsfull och korrekt hantering av informationssäkerhetsincidenter	Ja	Verksamhetsanalys	Rutinbeskrivning för LIS, processer för incidenthantering.
16.1.2 Rapportering av informationssäkerhetshändelser	Informationssäkerhetshändelser bör rapporteras genom lämpliga rapporteringsvägar så snabbt som möjligt	Ja	Verksamhetsanalys	Rutinbeskrivning för LIS, processer för incidenthantering.
16.1.3 Rapportering av svagheter gällande informationssäkerhet	Anställda och leverantörer som använder organisationens informationssystem och -tjänster bör vara skyldiga att notera och rapportera alla observerade eller misstänkta svagheter gällande informationssäkerhet i system eller tjänster	Ja	Riskanalys	Leverantörsavtal och bilagor, Förhållningsregler för serverhallen, Affärsverken IT-säkerhetsinstruktion.
16.1.4 Bedömning av och beslut om informationssäkerhetshändelser	Informationssäkerhetshändelser bör bedömas och beslut bör fattas om de klassificeras som informationssäkerhetsincidenter	Ja	Verksamhetsanalys	Affärsverken IT-Säkerhetsinstruktion.
16.1.5 Hantering av informationssäkerhetsincidenter	Informationssäkerhetsincidenter bör hanteras i enlighet med dokumenterade rutiner	Ja	Verksamhetsanalys	Process för incidenthantering. Support IT och Driftsprocess IT. Affärsverken IT-säkerhetsinstruktion.
16.1.6 Att lära av informationssäkerhetsincidenter	Kunskaper baserade på analyser av hanterade informationssäkerhetsincidenter bör användas för att minska sannolikheten eller påverkan av framtida incidenter	Ja	Verksamhetsanalys	Avikelsehanteringsprocessen.
16.1.7 Insamling av bevis	Organisationen bör fastställa och tillämpa rutiner för identifiering, insamling, kopiering och bevarande av information som kan tjäna som bevis	Ja	Verksamhetsanalys	Avvikelsehanteringsprocessen.
17.1.1 Planering av kontinuitet för informationssäkerhet	Organisationen bör fastställa sina krav på informationssäkerhet och kontinuitet för styrning av informationssäkerhet vid svåra situationer, exempelvis under en kris eller katastrof	Ja	Verksamhetsanalys	Fastställda säkerhetsåtgärder enligt riskbedömning. Se, Krishanteringsprocess och checklistor.
17.1.2 Införa kontinuitet för informationssäkerhet	Organisationen bör fastställa, dokumentera, införa och upprätthålla processer, rutiner och säkerhetsåtgärder för att säkerställa den nivå av kontinuitet för informationssäkerhet som krävs vid en svår situation	Ja	Verksamhetsanalys	Fastställda säkerhetsåtgärder enligt riskbedömning. Se, Krishanteringsprocess och checklistor.

17.1.3 Styra, granska och utvärder kontinuitet för informationssäkerhet	Organisationen bör verifiera de fastställda och införda säkerhetsåtgärderna för kontinuitet för informationssäkerhet med jämna mellanrum för att säkerställa att de är giltiga och verkningsfulla under störningar	Ja	Verksamhetsanalys	Systematisk riskbedömning och kontroll inom LIS för serverhallen.
17.2.1 Tillgänglighet för informationsbehandlingsresurser	Informationsbehandlingsresurser bör vid införande ha tillräcklig redundans för att uppfylla krav på tillgänglighet	Ja	Riskanalys	Säkerhetsåtgärder enligt riskbedömning, Krishanteringsprocess och checklistor.
18.1.1 Identifiering av gällande lagstiftning och avtalsmässiga krav	Alla relevanta författningsenliga och avtalsmässiga krav samt organisationens tillvägagångssätt för att uppfylla dessa krav bör uttryckligen identifieras, dokumenteras och hållas uppdaterade för varje informationssystem och organisationen	Ja	Omvärldsanalys - Rättsliga krav	Systematisk omvärldsbevakning och kontroll inom LIS för serverhallen.
18.1.2 Immateriella rättigheter	Lämpliga rutiner bör införas för att säkerställa efterlevnad av författningsenliga och avtalsmässiga krav relaterade till immateriella rättigheter och användning av proprietär programprodukter	Ja	Omvärldsanalys - Rättsliga krav	Systematisk omvärldsbevakning och kontroll inom LIS för serverhallen.
18.1.3 Skydd av dokumenterad information	Dokumenterad information bör skyddas från förlust, förstörelse, förfalskning, obehörig åtkomst och otillåten utgivning i enlighet med författningsenliga, avtalsmässiga och verksamhetsmässiga krav	Ja	Riskanalys	Säkerhetsåtgärder enligt klassning och riskbedömning
18.1.4 Skydd av personlig integritet och personuppgifter	I förekommande fall bör skydd av personlig integritet och personuppgifter säkerställas i enlighet med gällande författningar	Ja	Omvärldsanalys - Rättsliga krav	Rutiner för personuppgiftshantering, Integritetspolicy.
18.1.5 Regler av kryptografiska säkerhetsåtgärder	Kryptografiska säkerhetsåtgärder bör användas i enlighet med alla gällande avtal och författningar	Nej	Verksamhetsanalys	Ej relevant.
18.2.1 Oberoende granskning av informationssäkerhet	Organisationens tillvägagångssätt för att hantera informationssäkerhet och dess införande (d.v.s. mål, säkerhetsåtgärder, regler, processer och rutiner för informationssäkerhet) bör med jämna mellanrum eller när betydande förändringar sker genomgå oberoende granskning	Ja	Verksamhetsanalys	ISO 27001-certifiering med årlig extern revision.

18.2.2 Efterlevnad av säkerhetspolicy, regler och standarder	Högsta ledningen bör inom gällande ansvarsområden regelbundet granska efterlevnaden av informationssäkerhetspolicyn, gällande regler och riktlinjer, standarder och eventuella andra säkerhetskrav i förhållande till informationsbearbetning och rutiner	Ja	Verksamhetsanalys	LIS för Serverhallen.
18.2.3 Granskning av teknisk efterlevnad	Informationssystem bör granskas regelbundet avseende efterlevnad av organisationens informationssäkerhetspolicy, regler, riktlinjer och standarder	Ja	Verksamhetsanalys	Systematisk riskbedömning och kontroll inom LIS för serverhallen, interna revisioner, ledningsgenomgångar.