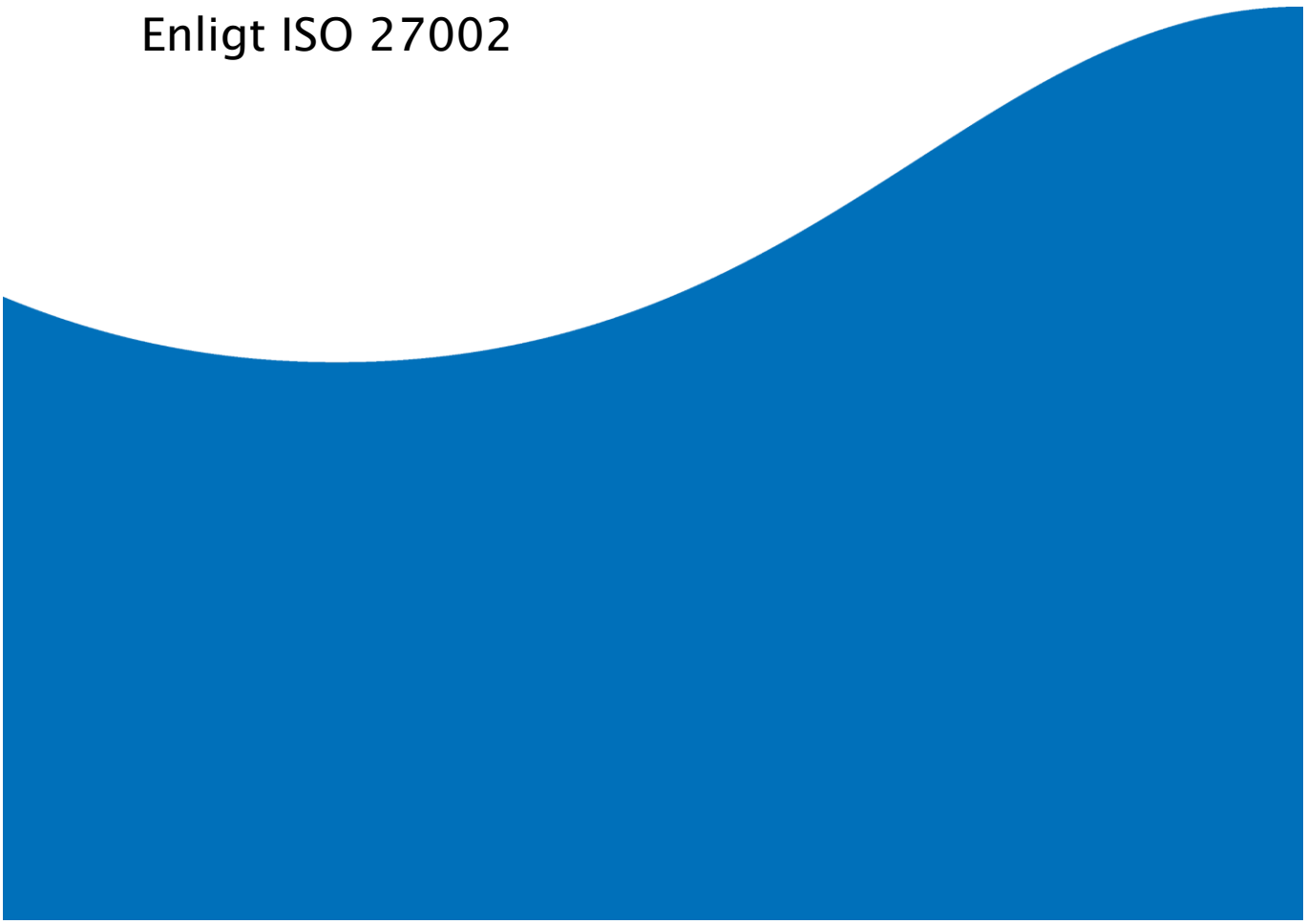
KARLSBORG

Riktlinje för informationssäkerhetsåtgärder

Enligt ISO 27002



Gäller för:	Samtliga förvaltningar och bolag
Diarienummer:	2023-349
Beslutande:	Kommunstyrelsen
Datum för beslut:	2023-10-11
Paragraf i protokoll:	137
Gäller från och med:	2023-11-01
Dokumentansvar:	Kanslichef
Aktualitetsprövning:	Ska ske under första året av varje mandatperiod.

Innehåll

INLEDNING 4

LEDNINGSSYSTEM FÖR INFORMATIONSSÄKERHET 4
Informationssäkerhetspolicy och andra styrdokument 4
Granskning av regelverk för informationssäkerhet 4

ORGANISATION AV INFORMATIONSSÄKERHETSARBETET 5
Informationssäkerhetsroller och ansvar 5
Kontakt med myndigheter 5
Regler för mobila enheter 5
Distansarbete 6

PERSONALSÄKERHET 6
Bakgrundskontroller 6
Anställningsvillkor 7
Ledningens ansvar 7
Medvetenhet, utbildning och fortbildning vad gäller informationssäkerhet 7
Disciplinär process 7
Avslut eller ändring av anställds ansvar 7

HANTERING AV INFORMATIONSTILLGÅNGAR 8
Inventering av informationstillgångar 8
Ägarskap av tillgångar 8
Klassning av information 8
Märkning av information 9
Hantering av tillgångar (användarinstruktioner) 9
Hantering av flyttbara lagringsmedia 9
Avveckling av lagringsmedia 9

STYRNING AV ÅTKOMST 10
Regler för styrning av åtkomst 10
Registrering och avregistrering av användare 10

Tilldelning av användaråtkomst 10
Hantering av priviligierade åtkomsträttigheter 10
Hantering av användares konfidentiella autentiseringsinformation 11
Granskning av användares åtkomsträttigheter 11
Borttagning eller justering av åtkomsträttigheter 11
Användning av konfidentiell autentiseringsinformation 12
Säkra inloggningsrutiner 12
System för lösenordshantering 12

FYSISK OCH MILJÖRELATERAD SÄKERHET 12
Fysiska tillträdesbegränsningar 12
Skydd mot yttre och miljörelaterad hot 13
Regler om rent skrivbord och tom skärm 13

DRIFTSÄKERHET 13
Dokumenterade driftsrutiner 13
Ändringshantering 13
Säkerhetsåtgärder mot skadlig kod 14
Säkerhetskopiering av information 14
Loggning av händelser 14
Synkronisering av tid 15

KOMMUNIKATIONSSÄKERHET 15
Säkerhetsåtgärder för nätverk 15
Regler och rutiner för informationsöverföring 15

ANSKAFFNING, UTVECKLING OCH UNDERHÅLL AV SYSTEM 15
Analys och specifikation av informationssäkerhetskrav 16
Rutiner för hantering av systemändringar 16
Teknisk granskning av tillämpningar efter ändringar i driftsmiljön 16
Skydd av testdata 17

HANTERING AV INFORMATIONSSÄKERHETSINCIDENTER 17
Ansvar och rutiner 17

Rapportering av informationssäkerhetshändelser....17
Rapportering av svagheter gällande informationssäkerhet....18
Att lära av informationssäkerhetsincidenter....18

INFORMATIONSSÄKERHETSASPEKTER AVSEENDE HANTERING AV VERKSAMHETENS KONTINUITET....18
Införa kontinuitet för informationssäkerhet....18

EFTERLEVNAD – GRANSKNING....18
Identifiering av gällande lagstiftning och avtalsmässiga krav....19
Skydd av personlig integritet och personuppgifter....19
Oberoende granskning av informationssäkerhet....19
Efterlevnad av säkerhetspolicy, regler och standarder....19
Granskning av teknisk efterlevnad....19

Inledning

ISO 27002:2017 och 27001:2017 riktar sig till svenska organisationer och deras arbete med informationssäkerhet. Att följa standarden är obligatoriskt för statliga myndigheter, men inte för kommuner. Men genom att ändå basera informationssäkerhetsarbetet på standardens kravområde ger en bra kvalitetsstämpel på arbetet.
Riktlinje för informationssäkerhetsåtgärder går igenom ISO-standarden 27001 och 27002´s kravområde och förtydligar vad dessa innebär för Karlsborg. Kravområdena genomlyses i en GAP-analys. I de område där kraven inte helt uppfylls ska beslut om åtgärd fattas. Endast ett urval av kravområdena ingår i GAP-analysen.

Ledningssystem för informationssäkerhet

Målet är att ledningssystemet ska delge ledningens inriktning och stöd för informationssäkerhet i enlighet med verksamhetens krav.

Informationssäkerhetspolicy och andra styrdokument

Ett regelverk för informationssäkerhet, där informationssäkerhetspolicyn är styrande, bör beslutas av högsta ledning och implementeras i alla verksamheter. Regelverket ska vara grundplåten i ledningssystem för informationssäkerhet. Andra delar kan tex åtgärdsplaner, utbildningsplaner och andra handlingsplaner.

Granskning av regelverk för informationssäkerhet

Regelverket (ledningssystemet) bör granskas med planerade intervaller eller om betydande förändringar sker. Granskningen ska säkerställa att regelverket fortsatt är lämpligt, riktigt och har önskad verkan på informationssäkerheten. Varje styrdokument har en dokumentansvarig. I dokumentansvaret ingår det att regelbundet granska och revidera dokumentet.

Även externa granskningar bör genomföras regelbundet.

Organisation av informationssäkerhetsarbetet

Målet är att upprätta ett ramverk för att det systematiska informationssäkerhetsarbetet ska fungera inom organisationen samt att säkerheten vid distansarbete och med mobila enheter säkerställs.

Informationssäkerhetsroller och ansvar

Informationssäkerhetspolicyn förtydligar hur organisationen av informationssäkerhetsarbetet är uppdelat och vilka roller som har vilket ansvar. Ibland kan det vara nödvändigt att ytterligare förtydliga vad som ligger i en rolls ansvar. Informationssäkerhetssamordnaren (kanslichef) har det övergripande ansvaret för att stötta verksamheterna i det systematiska informationssäkerhetsarbetet. Verksamheterna har ansvar för att se till att det finns tillgängliga resurser för arbetet och att verksamhetens medarbetare har tillräcklig kompetens.

Kontakt med myndigheter

Organisationen bör ha rutiner som anger när och av vem myndigheter (tex brottsbekämpande myndigheter och tillsynsmyndigheter mfl) bör kontaktas och hur identifierade informationssäkerhetsincidenter bör rapporteras vid lämplig tidpunkt. Att upprätthålla dessa kommunikationskanaler kan vara ett stöd vid tex attacker, andra incidenter eller vid kontinuitetsplanering av verksamheten.

Regler för mobila enheter

Mobila enheter är tex laptop, smartphone och surfplattor. När information lagras på denna typ av media krävs det att användaren iakttar extra försiktighet. Detta eftersom tex en smartphone, surfplatta eller laptop kan anslutas till nätverk som är publika, användas i publika miljöer och det är större risk att de förloras eller stjäls. För att minimera riskerna med mobila enheter ska de vara skyddade med lösenord eller liknande, uppsatta säkerhetsinställningar i enheten får inte ändras och multifaktorsinlogg (MFA) ska krävas då enheten ansluts till annat nätverk än den

kommunen tillhandahåller. Vid distansarbete ska endast utrustning som tillhandahållits av kommunen användas.

Se även rutin för dokumentlagring.

Distansarbete

Det bör finnas regler för hur information ska skyddas när medarbetare jobbar från distansarbetsplatser. Det bör även framgå vilken typ av utrustning som får användas, reglering kring uppkoppling på privata eller publika nätverk, krav på skydd mot skadlig kod och tillgång till fjärrskrivbord.

Personalsäkerhet

Målet är att anställda och leverantörer förstår sitt ansvar och är lämpliga för de roller de är anställda/anlitade för. Att de även är medvetna om och uppfyller sitt ansvar för verksamhetens informationssäkerhet. Att organisationens information är skyddad även efter att en anställning upphört.

Bakgrundskontroller

Bakgrundskontroll av sökande till tjänster i Karlsborgs kommun ska ske genom verifiering av den sökandes meritförteckning, tex genom kontakt med referenser och bekräftelse av påstådda akademiska och yrkesmässiga kvalifikationer. Kontroll av identitetshandling och påstådda yrkeslegitimationer (inom tex hälso- och sjukvården och läraryrkena) ska också genomföras.

För vissa kritiska tjänster krävs en förstärkt kontroll (tex kontroll av brottsregister mm). Sådana kritiska tjänster är tex kommunchef, förvaltningschef och personer som kommer få tillgång till känslig eller samhällsviktig information.

Den som genom en anställning eller på annat sätt ska delta i säkerhetskänslig verksamhet ska säkerhetsprövas enligt Säkerhetsskyddslagen (2018:585) innan anställningen påbörjas. De kontroller som genomförs framgår av Karlsborgs kommuns säkerhetsskyddsanalys/plan. Registerkontrollen administreras av säkerhetschef.

Alla bakgrundskontroller ska ta hänsyn till gällande lagstiftning rörande hantering av personuppgifter.

Anställningsvillkor

Nyanställda ska delges information om ansvar och skyldigheter kopplade till informationssäkerhet. I anställningen ska det tydligt framgå att den anställde förbinder sig att följa de styrande lagar, förordningar och andra styrande dokument som gäller för anställningen. Den nyanställde ska få tillgång till information m sekretess och ska skriva på en sekretessförbindelse för att påminna och tystnadsplikten.

Ledningens ansvar

Kommunens ledning ska se till att alla anställda har förutsättningar att följa de informationssäkerhetskrav som ställs på medarbetarna. Ledningen bör visa sitt stöd för policy för informationssäkerhet och tillhörande styrdokument. Ledningen ska upprätthålla lämpliga kunskaper och kvalifikationer i ämnet informationssäkerhet. Ledningen ansvarar för att tillhandahålla en anonym rapporteringskanal samt rutiner kring hantering av dessa ärende (sk whistleblow-funktion).

Medvetenhet, utbildning och fortbildning vad gäller informationssäkerhet

Vid introduktion av nya medarbetare ska de göras medvetna om det ansvar som anställningen innebär kopplat till informationssäkerhet. Alla medarbetare och i förekommande fall externa leverantörer ska erhålla lämplig utbildning för att kunna efterleva kommunens krav på informationssäkerhet. Roller som har särskilda uppgifter inom informationssäkerhet ska få fortbildning inom området som är lämplig för befattningen. Ett utbildnings- och introduktionsprogram bör fastställas för att säkerställa kontinuerlig och anpassad utbildning för samtliga medarbetare.

Disciplinär process

Arbetsrättsliga åtgärder kan behöva vidtas då anställda brutit mot gällande informationssäkerhetsregler. Närmaste chef ska med stöd från HR-enheten hantera dessa ärende på samma sätt som andra ärende gällande misskötsamhet.

Avslut eller ändring av anställds ansvar

Ansvar och skyldigheter för informationssäkerhet som förblir gällande efter avslut eller ändring av anställning ska definieras och kommuniceras vid anställningstillfället. Återlämnande av IT-utrustning ska ske i direkt samband med avslut eller ändring av

anställning. Närmste chef ansvarar för att avsluta anställningen och att avbeställa behörigheter, passerkort, nycklar och SITHS-kort så snart anställningen upphör. Information som den anställde producerat under anställningstiden har närmaste chef ansvar för att tillvarataga.

Hantering av informationstillgångar

Målet är att identifiera organisationens informationstillgångar och fastställa ansvar för att på så sätt skydda dem på en lämplig nivå samt att förhindra obehöriga åtgärder (röjande, modifierande, avlägsnande och destruktion).

Inventering av informationstillgångar

Samtliga informationstillgångar ska identifieras och inventeras. En uppdaterad förteckning ska finnas tillgänglig i Stratsys informationssäkerhetsmodul. Det ska finnas rutiner för hur denna förteckning ska hållas uppdaterad och vem som har ansvar för det.

Ägarskap av tillgångar

Samtliga informationstillgångar ska ha en ägare. För verksamhetssystem tilldelas en systemansvarig inom Karlsborgs kommun samt en teknikansvarig inom Skövde kommuns IT-enhet. Andra informationstillgångar tex nätverksutrustning, servrar odyl har Skövde kommuns IT-enhet ansvar och ägarskap för.

Klassning av information

Den data (information) som finns i kommunens informationstillgångar ska klassas enligt Karlsborgs kommuns fastställda modell för informationsklassning (se riktlinje för systematiskt informationssäkerhetsarbete). Resultatet av klassningen ger en bild av informationens värde beroende på deras känslighet och betydelse för verksamheten och därmed över hur avancerat skydd informationen behöver ha.

Målet är att hitta rätt nivå. Om informationstillgången klassas för högt finns risk att tillgången får för avancerade säkerhetsåtgärder, vilket kan leda till onödigt höga kostnader och krångliga rutiner. Om informationstillgången klassas för lågt finns det risk att informationen inte hanteras på ett korrekt sätt där konfidentialitet, riktighet och tillgängligheten äventyras.

Märkning av information

Klassningen utifrån konfidentialitet, riktighet och tillgänglighet ska mynna ut i en informationsmärkning som tydliggör informationstillgångens skyddsvärde. Modellen för informationsmärkning finns beskriven i riktlinje för systematiskt informationssäkerhetsarbete. Märkning av information är en viktig förutsättning för utbyte av information. Fysiska stämplar eller elektroniska metadata är vanliga former av märkning.

Hantering av tillgångar (användarinstruktioner)

Det ska finnas rutiner och instruktioner för hur informationstillgången får användas. Rutinerna och instruktionerna ska baseras på informationstillgångens klassning och skyddskrav. Personer som har tillgång till informationen ska veta hur den ska hanteras utifrån konfidentialitet, riktighet och tillgänglighet. Systemansvarig ansvarar för att se till att användarinstruktioner finns samt att utbildning sker. Användarinstruktionerna ska bla innehålla regler kring inloggning och lösenordshantering, behörighetsstrukturer, instruktioner för hur känslig information ska hanteras, information om vad som loggas och hur incidenter ska rapporteras.

Hantering av flyttbara lagringsmedia

Flyttbar lagringsmedia är tex USB-minnen, minneskort i kameror och externa hårddiskar ska endast användas i undantagsfall. Känslig och viktig information får inte lagras på denna typ av media. Om flyttbar lagringsmedia ändå anses nödvändiga ska de lösenordskyddas. Viktig information måste kopieras till annan (nätverks- eller serverbaserad) lagringsyta. Verksamheterna har ansvar för att hålla uppsikt över flyttbar lagringsmedia och förvara dem på ett säkert sätt.

Avveckling av lagringsmedia

Huvudregeln är att vid anställningens upphörande ska lagringsmedia återlämnas till närmaste chef. Möjlighet till att köpa ut tex surfplatta, telefon eller dator medges ej. Om utrustningen är för gammal ska den avvecklas/destrueras enligt gällande rutiner. Detta för att minimera risken att information som fortfarande finns lagrad på enheten inte blir tillgänglig för fel personer.

Styrning av åtkomst

Styrning av åtkomst handlar om att styra (begränsa eller tillåta) vem som har tillgång till vilken information. Målet är att rätt person ska ha rätt typ av åtkomst (behörighet) genom att på ett systematiskt sätt arbeta med behörighetstilldelning och att medarbetare är informerade om vad som gäller för den information de får tillgång till.

Regler för styrning av åtkomst

Det ska finnas beslutade och dokumenterade rutiner för behörighetshantering. Det är It-enhet eller systemansvarig som oftast tilldelar behörigheter och sätter strukturen för hur behörigheter ska tilldelas. Det kan även i onboardningprocessen finnas generella regler för vilka yrkesgrupper som ska åtkomst/behörighet till olika informationstillgångar.

Registrering och avregistrering av användare

Närmaste chef ansvarar för att beställa användarkonto till en medarbetare. Alla användare ska ha en unik användaridentitet. Namn på användare, tex e-postadresser, ska vara enhetliga för kommunen och stämma överens med namnuppgift i folkbokföringen. Gruppidentiteter är ej tillåtna.

Tilldelning av användaråtkomst

Användaråtkomst, eller behörighet, definierar vad en användare har rätt att utföra i systemet, tex läsa, skriva, radera eller skapa information. Grundprincipen är att behörighetstilldelning ska baseras på användarens behov till information i de informationstillgångar som behörighet ska tilldelas. Behoven kopplas till de uppgifter som användaren ska utföra i sitt uppdrag. Rutiner för hur tilldelning av behörigheter bör upprättas, efterlevas och följas upp.

Hantering av priviligierade åtkomsträttigheter

Priviligierade åtkomsträttigheter handlar om användarkonton med sk systembehörighet eller administrationsrättigheter. Denna typ av åtkomst bör få extra uppmärksamhet då rättigheterna medger tillgång till stor mängd information samt möjlighet till att ändra i systemet. Priviligierad åtkomsträttighet ska endast ges där det

uttryckligen är nödvändig och om möjligt ska rättigheterna vara tidsbegränsade. Priviligierade åtkomsträttigheter bör tilldelas ett användarkonto som skiljer sig från de konton som används för ordinarie verksamhet. Kompetensen hos användare med priviligierade åtkomsträttigheter bör ses över regelbundet för att verifiera att den är i nivå med arbetsuppgifterna. Granskning av priviligierade åtkomsträttigheter ska ske regelbundet.

Hantering av användares konfidentiella autentiseringsinformation

Lösenord är en vanligt förekommande typ av konfidentiell autentiseringsinformation och är ett vanligt sätt att verifiera en användares identitet. Andra exempel på konfidentiell autentiseringsinformation är fingeravtryck, ansiktsigenkänning, kryptografiska nycklar eller smarta kort (tex SITHS-kort).

Tilldelning av konfidentiell autentiseringsinformation bör styras genom en formell hanteringsprocess. Användaren bör får upplysning om hur autentiseringsinformationen ska hanteras.

Granskning av användares åtkomsträttigheter

Regelbunden uppföljning och revision av användares åtkomsträttigheter ska ske kontinuerligt. Extra uppmärksamhet ska ges till de konton/användare med priviligierade åtkomsträttigheter. När medarbetare avslutar eller byter tjänst är ett ypperligt tillfälle att se över åtkomsträttigheter. Rutiner för denna typ av kontroller ska finnas dokumenterade.

Borttagning eller justering av åtkomsträttigheter

Åtkomst som inte längre behövs ska tas bort snarast möjligt. När en medarbetare avslutar sin anställning ska användarkontot snarast avslutas. Det sätt som medarbetarens anställning avslutas kan vara avgörande för hur borttagning av åtkomsträttigheter hanteras. Om en medarbetare ofrivilligt avslutar sin anställning kan det finnas risk för att medarbetaren avsiktligt förvränger, raderar eller på annat sätt saboterar information.

Användning av konfidentiell autentiseringsinformation

Autentiseringsinformation ska hanteras som en värdehandling och får inte lämnas ut till någon. Lösenord mm ska förvaras på ett sådant sätt så att obehöriga inte kan komma åt den. Undvik att ha samma lösenord till flera olika inloggningar. Använd starka lösenord enligt den standard som är beslutad. SITHS-kort är en ID-handling och ska hanteras därefter

Säkra inloggningsrutiner

Säkra inloggningsrutiner bör användas i de system där det är fördelaktigt att kunna styrka den påstådda identiteten hos användaren. Olika system kan kräva olika typer av regler för inloggning. Styrkan på inloggningsrutinens säkerhet bör motsvara klassningsnivån som informationen har. En säker inloggningsrutin bör bland annat validera inloggningsinformation endast när all data matats in. Vid fel inloggningsinformation bör systemet inte ange vilken del av informationen som är rätt eller fel. Möjlighet att spåra misslyckade och lyckade inloggningar. Inte visa lösenordet i klartext. Automatiskt bli utloggad efter en viss tids inaktivitet

System för lösenordshantering

System för lösenordshantering kan underlätta att säkra inloggningsrutiner etableras. Sådana system kan bland annat säkerställa att lösenord av hög kvalitet väljs, lösenord byts ut med ett visst intervall, säkerställa att samma lösenord inte återanvänds mm.

Fysisk och miljörelaterad säkerhet

Målet är att skydda organisationens informationstillgångar och utrustning från otillåten fysisk åtkomst, miljörelaterade händelser samt illvilliga angrepp.

Fysiska tillträdesbegränsningar

Fysiska avgränsningar ska användas för att skydda utrymmen som innehåller informationstillgångar. Det kan vara olika typer av lås, larm och passagebehörigheter. Beroende på informationens klassning och märkning ska säkerhetsåtgärderna anpassas till en korrekt nivå. Ibland kan tillträdesloggar vara befogade.

Skydd mot yttre och miljörelaterad hot

Utrustning ska placeras och skyddas för att minska riskerna för miljörelaterade hot och möjlighet för obehörig åtkomst. Utrustningen ska underhållas korrekt och skyddas från elavbrott och andra störningar som kan orsaka fel i tekniska försörjningssystem. Godkänt brandskydd och brandlarm ska installeras. Medarbetare ska regelbundet få utbildning i hur släckningsutrustning ska hanteras. VA-dragningar i eller i direkt närhet av kritisk driftsutrustning ska undvikas. Strömkablar och telekommunikationskablar ska skyddas från avlyssning, störning och skada. Åtgärder ska vidtagas för att utrymme där driftsutrustning finns har rätt temperatur.

Regler om rent skrivbord och tom skärm

Rutin för att aldrig lämna känslig eller verksamhetskritisk information framme på skrivbordet (eller i olåst låda) ska finnas och följas. Papper och flyttbar lagringsmedia med känslig information ska förvaras i ett låst skåp. Rutin för att alltid låsa datorns skärm när den lämnas obevakad ska finnas och följas.

Driftsäkerhet

Målet är att säkerställa korrekt och säker drift av informationstillgångarna som ger skydd mot skadlig kod, förlust av data och där loggning sker regelbundet.

Driftsäkerhet handlar om att så långt det är möjligt undvika störningar och driftstopp i IT-miljön. För detta krävs att det finns rutiner för driftsättning, säkerhetskopiering och loggning. För Karlsborgs kommun gäller att Skövde kommun har ansvar för driften och dess säkerhetsfunktioner.

Dokumenterade driftsrutiner

Rutiner för drift av informationsbehandlings-och kommunikationsresurser bör finnas framtagna, dokumenterade och implementerade. Exempel på detta kan vara uppstarts- och nedtagningsrutiner, rutiner för säkerhetskopiering, rutiner för underhåll av utrustning, hantering av media och epost mm. Även rutiner för övervakning av informationstillgångar bör finnas för att upptäcka och åtgärda fel, minimera avbrott och förebygga IT-incidenter.

Ändringshantering

Förändringar i organisationen och dess verksamhetsprocesser sker hela tiden. När detta sker ska påverkan på IT-driften analyseras och testas för att kunna verifiera att informationssäkerhetskraven uppfylls även efter förändringen. Test- och

utbildningsmiljöer kan vara nödvändiga att sätta upp. Test-och utbildningsmiljöer har samma krav som ”skarp” IT-miljö när det gäller tex konfidentialitet på informationen.

Säkerhetsåtgärder mot skadlig kod

Skadlig kod är programvara, skript eller annan form av kod vars syfte är att skada (röja, förstöra, förvanska) informationstillgångar på ett obehörigt sätt. En organisation kan skydda sig om angrepp från skadlig kod (tex virus, maskar, trojaner, ransomware, spionprogram mm). Det finns tekniska åtgärder att vidtaga för att skydda organisationens information, såsom virusprogram, brandväggar, säkerhetsuppdateringar mm. Medarbetarnas kompetens är en typ av mänsklig brandvägg och är minst lika viktigt som den tekniska. Genom utbildning kan ledningen skapa en medvetenhet kring risker och en kultur som främjar säkert beteende

Säkerhetskopiering av information

Säkerhetskopiering av information och system är en viktig del av driftsäkerheten. Detta ger möjlighet att återställa en informationstillgång till ett fungerande tillstånd efter uppkomst av fel. Säkerhetskopieringen syfte till att viktig information ska kunna rekonstrueras med hjälp av kopior och återlagringsfunktioner. Säkerhetskopior ska lagras geografiskt åtskilt från originalmaterialet för att skydda mot fysiska incidenter (brand, översvämning mm). Det ska finnas rutiner för hur säkerhetskopiering av informationstillgångar ska gå till. Frekvens och omfattning av säkerhetskopieringen kan bero på klassningen av informationstillgången. Tester och övervakning av säkerhetskopiering ska ske regelbundet.

Loggning av händelser

Händelseloggar som registrerar användaraktiviteter ska regelbundet skapas, granskas och bevaras. Detta är viktigt för att kunna upptäcka fel, avvikelser och övriga informationssäkerhetsincidenter. Loggarna är även ett bra verktyg vid utredning av incidenter. Händelseloggarna kan bland annat innehålla uppgifter om användarkonto, systemaktiviteter, datum och tid för aktivitet, identifikation av använd enhet, lyckade och misslyckade inloggningsförsök, förändringar i systemkonfigurationen mm. Det är viktigt att tänka på att händelseloggar kan innehålla känslig information och själv loggen bör därför skyddas.

Verksamheten och ansvariga för IT-driften ska ha rutiner för hur loggning ska ske och hur informationen i loggen ska hanteras.

Synkronisering av tid

Systemklockorna i alla relevanta informationstillgångar ska vara synkroniserade mot en betrodd referenskälla för korrekt tid. Detta är viktigt bland annat för att säkerställa riktigheten av granskningsloggar.

Kommunikationssäkerhet

Målet är att säkerställa skyddet av information i nätverk och dess stödjande informationsbehandlingsresurser samt att upprätthålla säkerheten hos information vid överföring (inom organisationen eller extern)

Säkerhetsåtgärder för nätverk

Kommunikationssäkerhet är skydd i IT-resurser och nätverk som används för datakommunikation i syfte att skydda den information som kommuniceras. Nätverk måste hanteras och styras för att skydda information i anslutna system och tillämpningar. Det ska finnas rutiner för hantering av nätverk och förvaltning ska ske av ansvariga som utpekas av ägare till nätverk. Skyddsåtgärder ska införas för att nå säkerhet för information i nätverk och anslutna tjänster utifrån klassningen av anslutna objekt, dvs krav på konfidentialitet, riktighet och tillgänglighet. Krav på skydd ska inkluderas i avtal för nätverkstjänster om dessa tjänster tillhandahålls som outsourcade tjänster.

Regler och rutiner för informationsöverföring

Det ska finnas rutiner, regler och säkerhetsåtgärder för att skydda information vid överföring till annan part (intern eller extern). Regler för överföring ska spegla informationens klassning och märkning. Särskilt information som hanteras elektroniskt (e-post, lagring i moln, sociala medier mm) bör ges extra skydd.

Anskaffning, utveckling och underhåll av system

Målet är att säkerställa att informationssäkerhet är en integrerad del av informationstillgången över hela dess livscykel, från upphandling till avveckling.

Analys och specifikation av informationssäkerhetskrav

I ett införandeprojekt av ett nytt IT-system ska alltid informationssäkerhetsaspekten finnas som en del av kravställning mot leverantören. Kraven ska baseras på den klassning som tilldelats informationstillgången. Utveckling, anskaffning eller förändring av underliggande IT-resurser i form av infrastruktur, stödsystem med mera ska ha minst motsvarande krav som de system som de stöder. Ibland kan kraven vara ännu högre än för de system de stödjer, exempelvis om en IT-resurs stödjer ett stort antal system som var för sig inte är kritiska. Informationssäkerhetskrav ska dokumenteras och granskas av alla berörda parter innan utvecklingen, anskaffningen eller förändringen påbörjas.

På IT-system som driftas hos extern leverantör bör det ställas högre krav, tex leverantörens certifieringar, kontinuitetsplanering, rätt till tredjepartsrevision, sekretessavtal, PUB-avtal och rätt till incidentrapporter från leverantören.

Rutiner för hantering av systemändringar

Systemförändringar under en informationstillgångs livscykel bör styras genom användning av formella riktlinjer för ändringshantering. Säkerhet måste vara en integrerad del i utvecklingsprocessen, från början till slut.

För systemutvecklings- och integrationsåtgärder ska utvecklingsmiljöer upprättas och skyddas över IT-resursens hela livscykel. En säker utvecklingsmiljö inkluderar människor, processer och teknik som är involverad i systemutveckling och integration. Det innebär även att alla utvecklare måste ha en grundkompetens i programvarusäkerhet och att utvecklingsprocesser innehåller komponenter av utbildning och omvärldsbevakning.

Teknisk granskning av tillämpningar efter ändringar i driftsmiljön

Driftsmiljön omfattar operativsystem, databaser och mellanprogram. Säkerhetsåtgärden bör också tillämpas för ändringar av program.

När driftsmiljön ändras bör verksamhetskritiska tillämpningar granskas och testas för att säkerställa att det inte innebär någon negativ påverkan på verksamheten eller säkerheten.

Skydd av testdata

System- och acceptanstester kräver oftast stora volymer av testdata som så nära som möjligt överensstämmer med produktionsdata. Testdata bör noga väljas ut och skyddas för att undvika att testdatan innehåller personuppgifter eller annan konfidentiell information.

Hantering av informationssäkerhetsincidenter

Målet är att säkerställa ett konsekvent och verkningsfullt tillvägagångssätt för rapportering, hantering, bedömning och lärande av informationssäkerhetsincidenter.

Ansvar och rutiner

Alla användare, anställda och leverantörer ska göras medvetna om sin skyldighet att rapportera informationssäkerhetsincidenter. Det ska finnas tydliga rutiner och instruktioner om hur incidenter ska rapporteras. I de fall det rör sig om personuppgiftsincidenter ska även dataskyddsombud och eventuellt även Integritetsmyndigheten involveras.

Rapportering av informationssäkerhetshändelser

Incidentrapportering sker via Skövde kommuns serviceportal så snart som möjligt. Alla anställda kan rapportera händelser. Det förberedda formuläret ska fyllas i så snart som incidenten uppmärksammats. Notera detaljer om händelsen tex om brister i efterlevandet av rutiner, uppkomna tekniska fel, mänskliga fel, brister i fysiska skyddsåtgärder, fel i program eller hårdvara, felaktigheter i behörigheter och eventuella meddelanden på skärmen.

Rapportering av svagheter gällande informationssäkerhet

Svagheter i skyddet av informationstillgångarna kan ännu ej ha orsakat en incident, men det skulle mycke väl kunna hända något. Denna typ av svaghet (risk) ska också rapporteras i syfte att förebygga negativa konsekvenser.

Att lära av informationssäkerhetsincidenter

Rapporterade informationssäkerhetsincidenter ska sammanställas och analyseras i syfte att dra lärdom av händelserna. På så vis finns det möjlighet att anpassa rutiner eller utöka kompetens, för att undvika att samma eller liknande händer igen.

Informationssäkerhetsaspekter avseende hantering av verksamhetens kontinuitet

Målet är att kontinuiteten för informationssäkerhet bör vara integrerad i organisationens rutiner för kontinuitetshantering.

Införa kontinuitet för informationssäkerhet

Inom ramen för verksamhetens kontinuitets- och krishantering bör särskilda rutiner tas fram för hur informationssäkerheten bibehålls under extra ordinära händelser. Informationssäkerhetsåtgärder som införts bör fortsätta att fungera även under en störning. Om säkerhetsåtgärder inte kan upprätthålla skyddet bör andra åtgärder fastställas.

Efterlevnad – granskning

Målet är att undvika att bryta avtalsmässiga eller författningsenliga bestämmelser relaterat till informationssäkerhet samt att även interna styrdokument efterlevs.

Identifiering av gällande lagstiftning och avtalsmässiga krav

Ansvariga för organisationens olika IT-system ska löpande hålla sig uppdaterade på krav som återfinns i lagar, förordningar och avtal. Dessa krav ska dokumenteras för varje informationstillgång.

Skydd av personlig integritet och personuppgifter

I förekommande fall bör skydd av personlig integritet och personuppgifter säkerställas enligt gällande författningar, tex Dataskyddsförordningen. Organisationens personuppgiftsansvariga (nämnder och styrelser) ska vidtaga lämpliga tekniska och organisatoriska säkerhetsåtgärder för att skydda personuppgifter på rätt sätt. Skyddade personuppgifter är alltid konfidentiella och ska hanteras utifrån särskilda regler och rutiner.

Oberoende granskning av informationssäkerhet

Organisationens ledningssystem för informationssäkerhet bör regelbundet granskas av oberoende extern part, tex revisorer. Vid behov ska högsta ledningen inleda den oberoende granskningen. Granskningen ska svara på frågan om ledningssystemet är lämpligt, tillräckligt och verkningsfullt. Granskningen ska mynna ut i möjligheter till förbättringar.

Efterlevnad av säkerhetspolicy, regler och standarder

Högsta ledningen bör regelbundet initiera granskning av hur ledningssystemets styrdokument och handlingsplaner efterlevs och vilken effekt på verksamhetens informationssäkerhetsnivå arbetet får.

Granskning av teknisk efterlevnad

Granskning av de tekniska säkerhetskraven ska också granskas regelbundet. Detta kan göras med hjälp av automatiserade verktyg, manuella granskningar eller sk penetrationstester.