Riktlinje för informationssäkerhet

Antaget av: Kommunstyrelsen den 2022-05-30

Datum för revidering: 2026-06-01

Ansvarig för revidering: Kommunstyrelseförvaltningen

Diarienr.: KS 2022-195

Kapitel 1. Inledning

Informationssäkerhet omfattar skydd av all information oavsett form och innebär en strävan att skydda information så att:

- endast behöriga personer får ta del av informationen - konfidentialitet
- informationen går att lita på, att den är korrekt och inte manipulerad - riktighet
- informationen finns tillgänglig när den behövs - tillgänglighet

Konfidentialitet, riktighet och tillgänglighet utgör informationens egenskaper. Behovet av skydd utgörs av åtgärder som kan vara både av teknisk och administrativ natur.

Exempel på tekniska säkerhetsåtgärder är IT-säkerhet, fysisk säkerhet och datakommunikation, medan administrativ säkerhet är dokumentation, processer, analys, organisation, kompetensutveckling, efterlevnad, uppföljning samt ledning och styrning.

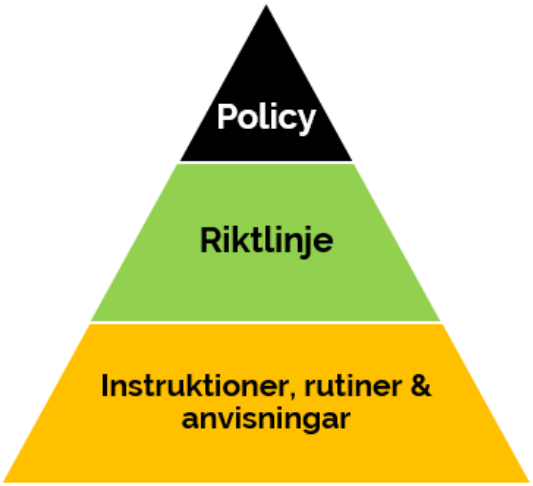
1.1 Syfte

Riktlinjen beskriver hur verksamheterna ska agera för att initiera, bibehålla och förbättra informationssäkerheten i kommunen.

Riktlinjen syftar till god och säker hantering av all information inom Nybro kommun, men också till ett aktivt och systematiskt informationssäkerhetsarbete så att rätt information finns tillgänglig för rätt personer vid rätt tidpunkt.

1.2 Omfattning

Riktlinjen för informationssäkerhet är underställd informationssäkerhetspolicyn. Beslutad policy och riktlinje utgör tillsammans med anvisningar, rutiner och instruktioner styrdokument för informationssäkerhet.



Riktlinjen för informationssäkerhet gäller för all verksamhet inom kommunen inklusive helägda bolag och omfattar alla informationstillgångar som kommunen hanterar.

Följande grupper omfattas av riktlinjen:

- samtliga anställda
- extern personal och politiker, vilka aktivt arbetar i verksamheten
- och politiker och elever, som ges tillgång till kommunens IT-nätverk

Med informationstillgång avses all information oavsett om den behandlas i ett IT-system, förekommer på ett utskrivet papper, i ett anteckningsblock, som ett samtal i korridoren eller i telefonen. Även film, ljud och bild inkluderas.

Riktlinjen baseras på svensk standard för informationssäkerhet. SS-ISO/IEC 27001:2017, som visar krav på informationssäkerhet och SS-ISO/IEC 27002:2017, som ger riktlinjer för informationssäkerhet.

Kraven på informationssäkerhet utgår från ledningens och verksamhetens krav på funktion och tillämplighet liksom legala krav, förordningar, föreskrifter, avtal och säkerhetskrav. Verksamheten förväntas ha tillräcklig kunskap om de lagar och förordningar som gäller för respektive område.

1.3 Termer och definitioner

Riktlinjen använder följande termer och definitioner.

Term	Definition
Autentisering	Kontroll av uppgiven identitet.
Behandling av personuppgifter	Varje åtgärd som någon vidtar med personuppgifter.
Behörighet	Tilldelad åtkomsträttighet till information/ IT-system.
Hot	Möjlig oönskad händelse med negativa konsekvenser för verksamheten.
Information	Ett vitt begrepp som inkluderar allt ifrån kunskap hos enskilda medarbetare till information lagrad i ett IT-system.
Informationstillgång	Med informationstillgång avses all information oavsett om den behandlas i ett IT-system, finns på ett utskrivet papper, i ett anteckningsblock, som ett samtal i korridoren eller i telefonen samt all form av film, ljud och bild.
Informationsrisk	Risk där konsekvensen påverkar konfidentialitet, riktighet eller tillgänglighet.
Informationssäker-hetspolicy	Övergripande avsikt och viljeinriktning formellt uttryckt av organisationens ledning. Anger inriktning för informationssäkerhetsarbetet inom organisationen.
IT-system	System som med informationsteknik (IT) hanterar information med omgivningen. I begreppet IT-system innefattas även datorer, kommunikationsutrustning, servrar, skrivare och övrig teknisk utrustning anslutna till kommunens nätverk.
Konfidentialitet	Att information inte görs tillgänglig eller avslöjas för obehöriga personer, enheter eller processer.
Känsliga personuppgifter	Uppgifter som avslöjar etniskt ursprung, politiska åsikter, religiös ellerfilosofisk övertygelse, medlemskap i fackförening samt uppgifter som rör hälsa eller sexualliv. Patientuppgifter är känsliga personuppgifter.
Mobil enhet	Mobiltelefon, surf- eller läsplatta, bärbar dator eller liknande digital enhet.
Personuppgifter	All slags information som direkt eller indirekt kan knytas till en fysisk person som är i livet. Bild- och ljuduppgifter om en identifierbar fysisk person räknas som personuppgift även om inga namn nämns.
Riktighet	Skydd mot oönskad förändring, att informationen går att lita på.

Risk	Produkten av sannolikhet och konsekvens för att ett givet hot realiseras.
Riskanalys	Metodisk aktivitet som identifierar,beskriver och värderar risk inom ett område.
Samtycke	Varje slag av otvetydig viljeyttring genom vilken den registrerade godtar att personuppgifter som rör honom eller henne behandlas.
SITHS-kort	Tjänstekort med elektronisk ID som används för autentisering vid inloggning till IT-system.
Skadlig kod	Otillåten programkod som syftar till att ändra, röja, förstöra, störa eller avlyssna ett datanät, funktioner eller uppgifter i IT-system.
Skyddsåtgärd	Handling, procedur eller teknisk aktivitet som minskar sårbarheten mot kända hot.
Stark autentisering	Autentisering som innebär att identiteten kontrolleras på minst två sätt.
Sårbarhet	Brist i skyddet av tillgångar exponerade för hot.
Tillgång	Något som har värde för en organisation. Med informationstillgångar menas information i sig och de resurser som används för att hantera den, till exempel programvaror, tjänster och fysiska tillgångar.
Tillgänglighet	Att vara tillgänglig och användbar för en behörig användare när man behöver den.

1.4 Struktur och läsanvisning

Läsanvisningen nedan syftar till att förklara riktlinjens innehåll och användning. Varje kapitel inleds med en kort sammanfattning som beskriver innehåll och syfte.

Kapitel		Innehåll	Sida
1	Inledning	ISO kap. 5 Allmän beskrivning samt informationspolicy	2 - 5
2	Styrning och ledning	ISO kap. 6 Organisation, med ansvar och roller.	6 - 8
3	Personalsäkerhet	ISO kap. 7 Före, under och efter anställning.	8 - 9
4	Hantering av tillgångar	ISO kap. 8 Förteckning och ägarskap för att säkra skydd av informationstillgångar.	10 - 11
5	Styrning av åtkomst	ISO kap. 9 Behörigheter, både logisk och fysisk, för att begränsa åtkomst till information.	11 - 12
6	Kryptering	ISO kap. 10 Krypteringsskydd av information.	13
7	Fysisk och miljörelaterad säkerhet	ISO kap. 11 Förhindra otillåten fysisk åtkomst, beskrivning över fysiskt skydd och lokalisering.	13 - 14
8	Driftsäkerhet	ISO kap. 12 Rutiner för korrekt och säker hanteringen av information.	15 - 17

9	Kommunikationssäkerhet	ISO kap.13 Hantering av information i nätverk och i dess resurser.	17
10	Anskaffning, utveckling och underhåll	ISO kap.14 Säkerställa informationskrav vid inköp, underhåll och utveckling.	18 - 19
11	Leverantöresrelationer	ISO kap. 15 Säkerställa skydd av information en leverantör kan ha tillgång till.	19
12	Hantering av informationssäkerhetsincidenter	ISO kap. 16 Säkerställa effektiv hantering av informationssäkerhetsincidenter.	20 - 21
13	Verksamhetens kontinuitet	ISO kap. 17 Kontinuitet ska vara en integrerad del i all verksamhet, bäring mot NIS.	21
14	Efterlevnad	ISO kap. 18 Undvika överträdelser av juridiska och avtalsmässiga krav.	22

1.5 Uppföljning

Dokumentet revideras enligt klassificeringsstrukturen, men aktualitetsförklaras vid förändringar och minst en gång per år.

Kapitel 2. Styrning och ledning

2.1 Roller och ansvar

Fokus: Organisationen för informationssäkerhetsarbetet ska stödja och styra införandet och förvaltningen av informationssäkerhetsarbetet i kommunen.

Kommunens har en upprättad organisation med utpekade roller och ansvar för informationssäkerheten. Ansvaret sträcker sig från den politiska ledningen, genom tjänstemannaledningen ner till varje enskild användare.

Politisk ledning

Den politiska ledningen har det övergripande ansvaret för informationssäkerhet. Kommunfullmäktige, kommunstyrelsen och respektive nämnders och bolagsstyrelsers ansvar för informationssäkerhetsarbetet beskrivs kortfattat nedan.

Roll	Ansvar
Kommunfullmäktige	Kommunfullmäktige fastställer policyn för informationssäkerhet, vilken uttrycker viljeinriktningen för kommunens arbete med informationssäkerhet.
Kommunstyrelsen	Kommunstyrelsen fastställer riktlinjen för informationssäkerhet och har det yttersta ansvaret för kommunens informationssäkerhetsarbete samt kommunstyrelsens verksamheter. Kommunstyrelsen utser Dataskyddsombud och är ytterst personuppgiftsansvarig för sina verksamheter.
Nämnden/bolagsstyrelsen	De kommunala nämnderna/styrelserna har ansvaret för informationssäkerhetsarbetet inom sina respektive verksamheter/myndigheter. Nämnden/styrelsen är ytterst personuppgiftsansvarig.

Roller och ansvar i verksamheten

Roll	Ansvar
Kommunchef	Ansvarar att tillse att informationssäkerhetsarbetet bedrivs så effektivt som möjligt, genom att visa ett tydligt stöd och fördela resurser.
Varje chef	Varje chef ansvarar för att det finns rutiner som säkerställer att underställda kan efterleva kommunens regelverk för informationssäkerhet.

Informationssäkerhets-samordnaren	Har det övergripande och strategiska ansvaret att leda, utveckla och samordna informationssäkerhetsarbetet samt föreskriva de metoder som skall använda för riskanalys och informationsklassning.
Informationsägare	Har ansvaret för den informationsmängd som delegerats dem, normalt den information som verksamheten hanterar. Informationsägarna har ansvar för att informationsklassning och riskanalyser genomförs för den informationsmängd som de ansvarar för. De har vidare ansvar att informationen hanteras på ett ändamålsenligt sätt inom de krav informationsklassningen ställer.
Systemägare	Har ansvar för respektive IT-system och dess användning. System ska uppfylla informationssäkerhetskraven i utifrån informationsklassificeringen och legala krav. Prioritering av resurser skall göras utifrån verksamhetens behov. Systemägarna ansvarar vidare att upprätthålla en god dokumentation över systemen.
Dataskyddsombud	Kommunen har skyldighet att tillsätta ett Dataskyddsombud med sakkunskap om lagstiftning och praxis om dataskydd. Rollen skall vara självständig, rådgivande och övervakande i att kommunen följer reglerna i Dataskyddsförordningen.
Övriga roller	Kommunens verksamhetsledning bestående av ledande tjänstemän har det organisatoriska ansvaret för arbetet med informationssäkerhet. Kommunchefen och förvaltningscheferna har särskilt ansvar för organisation, ledning och styrning av informationssäkerhetsarbetet.
Förvaltningschef	Förvaltningschef har på kommunchefens och nämndens uppdrag att tillse att informationssäkerhetsarbetet bedrivs så effektivt som möjligt genom att visa ett tydligt stöd och tilldela resurser. Förvaltningschefen utser ansvarig resurs för samordning av informationssäkerhetsarbetet inom sin förvaltning samt systemägare för övriga system. Anvisningar, rutiner och instruktioner fastställs av förvaltningschef eller efter delegation.
Chef för kommunala bolag	De kommunala bolagscheferna har på styrelsens uppdrag att tillse att informationssäkerhetsarbetet i bolaget bedrivs i enlighet med kommunens riktlinje för informationssäkerhet.
Systemförvaltare	Systemförvaltarens uppdrag är förvaltning och underhåll av systemet. Förvaltaren ska tillgodose att fastställd säkerhetsnivå upprätthålls.
IT-chef	IT-chefen ska leda och samordna informations-säkerhetsarbetet för kommunens IT-infrastruktur.

Uppdelning av ansvarsuppgifter
Ansvar och ansvarsområden som står i konflikt med varandra ska åtskiljas. Detta görs bl.a genom att definiera rollerna informationsägare, systemägare och systemförvaltare.

Kontakt med myndigheter
Lämpliga kontakter med relevanta myndigheter ska upprätthållas av respektive förvaltning/bolag/funktion.

Kontakt med särskilda intressegrupper
Lämpliga kontakter med särskilda intressegrupper eller andra forum för säkerhetsspecialister och branschorganisationer ska upprätthållas. Anpassas till den egna verksamheten.

Informationssäkerhet i projektledning
Informationssäkerhet ska hanteras inom projektledning, oavsett typ av projekt. Lämpligen någon form av riskanalys och engagemang av rätt kompetens tidigt i projekten.

2.2 Mobila enheter och distansarbete

Fokus: Att säkerställa säkerheten vid distansarbete och vid användning av mobila enheter.

Regler för mobila enheter
Regler och stödjande säkerhetsåtgärder ska antas för att hantera de risker som användning av mobila enheter så som laptop, mobiltelefon eller läsplatta medför.

Distansarbete
Regler och stödjande säkerhetsåtgärder ska införas för att skydda information som nås, bearbetas eller lagras på distansarbetsplatser, ofta hemmet med tanke på nuvarande situation.

Kapitel 3. Personalsäkerhet

Detta kapitel beskriver vad som görs i samband med rekrytering, anställning och avslutande av anställning.

3.1 Före anställning

Fokus: Att säkerställa att alla kandidater är lämpliga för de roller som de är tilltänkta för.

Bakgrundskontroll
Bakgrundskontroll på alla sökande för anställning ska utföras i enlighet med verksamhetskrav

och klassificeringen av information som de ges behörighet till. Identitetskontroll skall alltid göras.

Anställningsvillkor
Verksamheterna ska i anställningsvillkor inkludera ett uttalande om den anställdes ansvar för informationssäkerhet. Samtliga medarbetare ska göras medvetna om sina skyldigheter samt om gällande regler för informationssäkerhet och sekretess. Alla anställda och övriga berörda ska underteckna en sekretessförbindelse eller motsvarande.

Det ska vara tydligt vilken information som ägs av kommunen och att den inte får förstöras eller kopieras vid avslutande av anställning eller uppdrag.

3.2 Under anställning

Ledningens ansvar
Ledningen ska kräva att alla anställda och leverantörer tillämpar informationssäkerhetskrav i enlighet med för organisationen fastställda regler och rutiner.

Medvetenhet, utbildning och fortbildning i 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.

Disciplinära åtgärder
Det ska finnas en formell och kommunicerad disciplinär process för att vidta åtgärder mot anställda som har brutit mot gällande informationssäkerhetsregler.

3.3 Avslut eller ändring av anställning

Fokus: Att skydda Nybro kommuns intressen som en del av processen för att ändra eller avsluta en anställning.

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.

Kapitel 4. Hantering av tillgångar

4.1 Ansvar för tillgångar

Fokus: Att identifiera tillgångar och fastställa lämpligt ansvar för att skydda dem.

Inventering av tillgångar
Tillgångar i form av information och system för informationsbehandling ska identifieras och en förteckning över dessa tillgångar ska upprättas och underhållas.

Ägarskap av tillgångar
Tillgångar i förteckningen ska kopplas till ägare, Informationsägare och Systemägare.

Tillåten användning av tillgångar
Regler för tillåten användning av tillgångar ska identifieras, dokumenteras och införas. Användare ska göras medvetna om de krav på informationssäkerhet som gäller för tillgångarna.

Återlämnande av tillgångar
Tillgångar ska återlämnas då anställning, uppdrag eller avtal upphör, om inte särskild överenskommelse upprättas.

4.2 Informationsklassning

Klassning av information
Information ska klassas utifrån rättsliga krav, informationens värde för verksamheten och den enskilde. Informationsägaren ansvarar för att informationsklassning genomförs.

Märkning av information
Rutiner för märkning av information ska utvecklas och införas enligt informationsklassning på de enheter som tillåter märkning, typ laptop.

Hantering av tillgångar
Rutiner för hantering av tillgångar ska utvecklas och införas de krav informationsklassningen ställer.

4.3 Hantering av lagringsmedia

Fokus: Att förhindra obehörigt röjande, modifiering, avlägsnande eller destruktion av information som lagras på media.

Hantering av flyttbara lagringsmedia
Rutiner ska införas för hantering av flyttbara lagringsmedia. Användning av flyttbara lagringsmedia skall undvikas. Exempel är USB-minnen, externa hårddiskar, minneskort och kamera.

Avveckling av lagringsmedia
Lagringsmedia ska avvecklas när det inte längre behövs. Formella rutiner skall fastställas av informationsägare.

Transport av fysiska lagringsmedia
Lagringsmedia som innehåller information ska skyddas mot obehörig åtkomst, missbruk eller förvanskning under transport.

Kapitel 5. Styrning av åtkomst

Åtkomst till information, informationssystem och tjänster ska begränsas i enlighet med informationsägares krav.

5.1 Verksamhetskrav för styrning av åtkomst

Fokus: Korrekt åtkomst till information, informationssystem och tjänster.

Regler för styrning av åtkomst
Åtkomst till information ska regleras av informationsägaren. I de fall leverantör eller annan organisation hanterar kommunens information ska regler för styrning av åtkomst regleras i avtal.

Tillgång till nätverk och nätverkstjänster
Användare ska endast ges tillgång till de nätverk och nätverkstjänster som de beviljats åtkomst till.

5.2 Hantering av användaråtkomst

Fokus: Att säkerställa behörig användaråtkomst och att förhindra obehörig åtkomst till information, informationssystem och tjänster.

Registrering och avregistrering av användare
En formell process för registrering och avregistrering av användare ska finnas. Användare ska vara unikt identifierade. Gruppkonton för inloggning är inte tillåtna.

Tilldelning av användaråtkomst
En formell process för tilldelning av åtkomst ska finnas. Tillgång till alla informationssystem ska styras med hjälp av åtkomstkontroll.

Hantering av privilegierade åtkomsträttigheter ("Admin")
Åtkomst med utvidgade rättigheter, så kallade administratörsrättigheter, ska begränsas till så få personer som möjligt. Behörigheter ska vara begränsade till vad som krävs för att utföra de arbetsuppgifter användaren har. Samma identitet ska inte användas för systemadministration och vanlig användning.

Hantering av användares konfidentiella autentiseringsinformation
Hantering av användares inloggningsuppgifter som t.ex. lösenord, PIN-koder och SITHS-kort, ska ske på ett sådant sätt att uppgifterna inte röjs. Om dessa uppgifter röjs ska detta omgående anmälas.

Granskning av användares åtkomsträttigheter
Informationsägare ska granska användarnas åtkomsträttigheter periodiskt och/eller efter systemförändringar som kan påverka åtkomsträttigheterna.

Borttagning eller justering av åtkomsträttigheter
Åtkomsträttigheter till information och informationssystem ska tas bort vid avslutande av anställning,avtal eller uppdrag och justeras vid förändringar. Chef som är ansvarig för anställning, avtal eller uppdrag ansvarar för att hantera detta.

5.3 Användaransvar

Fokus: Att göra användare ansvariga för att skydda sina inloggningsuppgifter.

Användning av konfidentiell autentiseringsinformation
Hantering av inloggningsuppgifter som t.ex. lösenord, PIN-koder och SITHS-kort, ska ske på ett sådant sätt att uppgifterna inte röjs. Om dessa uppgifter röjs ska detta omgående anmälas.

5.4 Styrning av åtkomst till system och tillämpningar

Fokus: Att förhindra obehörig åtkomst till system och tillämpningar.

Begränsning av åtkomst till information
Tillgång till information och systemfunktioner ska vara begränsad enligt regler för åtkomst.

Säkra inloggningsrutiner
Tillgång till system och tillämpningar styras genom säkra inloggningsrutiner för att minimera risken för obehörig åtkomst. Information med hög konfidentialitet som t.ex. känsliga personuppgifter bör skyddas med stark autentisering.

System för lösenordshantering
System för lösenordshantering ska säkerställa kvalitativa lösenord. Riktlinjer för lösenord och autentisering skall finnas, kopplat till informationsklassning.

Användning av privilegierade verktygsprogram
Användning av program som kan ha förmåga att kringgå säkerhetsåtgärder i system och tillämpningar ska begränsas och styras strikt, helst undvikas.

Kapitel 6. Kryptering

Detta kapitel beskriver vad som ska omfattas och beaktas vid kryptering.

6.1 Kryptografiska säkerhetsåtgärder

Regler för användning av kryptering
Beslut om krypteringslösning ska tas om det bedöms som en lämplig säkerhetsåtgärd baserad på informationsklassning och riskbedömning.

Nyckelhantering
Rutiner för hantering av kryptografiska nycklar ska vara dokumenterad och belysa aspekter som hur nycklarna tas fram, hur de lagras och hur åtkomst ska ske.

Kapitel 7. Fysisk och miljörelaterad säkerhet

Detta kapitel beskriver vad som ska omfattas och beaktas angående fysisk och miljörelaterad säkerhetför informationssystem, informationstillgångar och tjänster i egna lokaler såväl som externa.

7.1 Säkra områden
Fokus: Att förhindra otillåten fysisk åtkomst till, skador på och störningar i tillgången till kommunens information, informationssystem och tjänster.

Fysiska säkerhetsavgränsningar
Fysiska avgränsningar ska definieras och användas för att skydda områden som innehåller antingen känslig eller kritisk information, informationssystem och tjänster.

Fysiska tillträdesbegränsningar
Säkra områden ska skyddas genom lämpliga säkerhetsåtgärder, t.ex. lås eller stängsel, för att säkerställa att endast behörig personal får tillträde.

Säkerställande av kontor, rum och anläggningar
Fysisk säkerhet för kontor, rum och anläggningar ska utformas och tillämpas.

Skydd mot yttre och miljörelaterade hot
Fysiskt skydd ska utformas och införas för att motverka effekterna av naturkatastrofer, illvilliga angrepp eller olyckor.

Arbeta i säkra utrymmen
Rutiner för arbete i säkra utrymmen ska finnas.

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. Likaså bör inkommande gods kontrolleras.

7.2 Utrustning
Fokus: Att förhindra förlust, skada, stöld eller påverkan av tillgångar och avbrott i kommunens verksamhet.

Placering och skydd av utrustning
Utrustning ska placeras och skyddas för att minska riskerna för miljörelaterade hot och faror och möjligheter för obehörig åtkomst.

Tekniska försörjningssystem
Utrustning ska skyddas från elavbrott och andra störningar som orsakas av fel i tekniska försörjningssystem.

Kablagesäkerhet
Kablage för ström, tele och datakommunikation ska skyddas från avlyssning, störningar och skada.

Underhåll av utrustning
Utrustning ska underhållas korrekt för att säkerställa fortsatt tillgänglighet och riktighet. Utrustning i detta avseende är primärt tekniska försörjningssystem.

Utförsel av tillgångar
Utrustning, information eller program ska inte avlägsnas utanför organisationens lokaler utan tillstånd.

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.

Säker kassering eller återanvändning av utrustning
All utrustning som innehåller lagringsmedia ska granskas för att säkerställa att all känslig data och licensierade program har avlägsnats eller säkert överskrivits före kassering eller återanvändning.

Obevakad utrustning som hanteras av användare
Användare ska säkerställa att obevakad utrustning har lämpligt skydd.

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.

Kapitel 8. Driftsäkerhet

Detta kapitel beskriver drift och underhåll av informationssystem.

8.1 Driftrutiner och ansvar

Fokus: Att säkerställa korrekt och säker drift av informationssystem och tjänster.

För att upprätthålla säker och tillförlitlig tillgång till information och funktion ska administration, drift och underhåll av informationssystem ske på ett strukturerat och systematiskt sätt.

Dokumenterade driftsrutiner

Det ska finnas systemdokumentation för varje informationssystem. Dokumentationen ska normalt bestå av system-, drift- och användardokumentation och omfatta all information som behövs för att informationssystemet ska kunna användas på ett säkert och korrekt sätt.

Ändringshantering

Förändringar i informationssystem och tjänster som påverkar informationssäkerheten ska styras.

Kapacitetshantering

Användningen av resurser ska övervakas samt vid behov justeras. Prognoser av framtida kapacitetskrav ska göras för att säkerställa nödvändig systemprestanda.

Separation av utvecklings-, test- och driftmiljöer

Produktionsmiljöer för verksamhetskritiska system ska vara separerade från övriga miljöer t.ex. utvecklings-, test- och utbildningsmiljöer för att minska risken för obehörig åtkomst eller ändringar i produktionsmiljön.

8.2 Skydd mot skadlig kod

Fokus: Att säkerställa att information, informationssystem och tjänster skyddas mot skadlig kod.

Säkerhetsåtgärder mot skadlig kod

Upptäckande, förebyggande och återställande säkerhetsåtgärder för att skydda mot skadlig kod ska finnas, i kombination med säkerställande av en lämplig nivå av medvetenhet hos användarna.

8.3 Säkerhetskopiering

Fokus:: Att skydda mot förlust av data

Säkerhetskopiering av information

Säkerhetskopior av information, program och speglingar av system ska tas och testas regelbundet i enlighet med överenskomna regler och krav för säkerhetskopiering.

8.4 Loggning och övervakning

Syfte: Att logga händelser och ev. säkra bevis för otillåten aktivitet.

Loggning av händelser
Händelseloggar som registrerar användaraktiviteter, avvikelser, fel och informationssäkerhetshändelser, ska skapas, bevaras och granskas regelbundet. Det är informationsägarens ansvar att ställa krav så att loggning sker och sparas i enlighet med det aktuella informationssystemet.

Skydd av logginformation
Loggarna ska vara skyddade mot obehörig åtkomst och manipulation.

Administratörs- och operatörsloggar
Systemadministratörers och systemoperatörers aktiviteter ska loggas och loggarna ska skyddas och granskas regelbundet.

Synkronisering av tid
Systemklockorna i alla relevanta informationssystem och tjänster ska synkroniseras mot en och samma referenskälla för tid.

8.5 Styrning av driftsystem

Fokus: Att säkerställa riktigheten hos driftsystem.

Installation av program på driftsystem
Rutiner ska finnas för att styra installation av programvara på driftsystem.

8.6 Hantering av tekniska sårbarheter

Fokus: Att förhindra utnyttjande av tekniska sårbarheter.

Hantering av tekniska sårbarheter
Information om tekniska sårbarheter i de informationssystem som används ska erhållas i tid, organisationens exponering för sådana sårbarheter ska analyseras och lämpliga åtgärder vidtas för att behandla den tillhörande risken.

Restriktioner för installation av program
Regler för programinstallationer som utförs av användare ska upprättas och införas.

8.7 Överväganden gällande revision av informationssystem

Fokus: Att minimera revisionsverksamhetens påverkan på informationssystem.

Revisionskontroller för informationssystem
Revisionskrav och revisionsaktiviteter på driftsystem ska planeras noggrant och godkännas, för att minimera störningar i verksamhetsprocesser.

Kapitel 9. Kommunikationssäkerhet

Detta kapitel beskriver vad som ska omfattas och beaktas vid kommunikations- och nätverkssäkerhet.

9.1 Hantering av nätverkssäkerhet

Fokus: Att säkerställa skyddet av information i nätverk och dess stödjande informationssystem och tjänster.

Säkerhetsåtgärder för nätverk
Nätverk ska hanteras och styras för att skydda information i system och tillämpningar.

Säkerhet hos nätverkstjänster
Säkerhetsmekanismer, tjänstenivåer och ledningskrav vad gäller alla nätverkstjänster ska identifieras och inkluderas i avtal för nätverkstjänster, oavsett om dessa tjänster tillhandahålls internt eller som outsourcade tjänster.

Separation av nätverk
Grupper av informationstjänster, användare och informationssystem ska separeras i nätverk.

9.2 Informationsöverföring

Fokus: Att upprätthålla säkerheten hos information som överförs inom kommunen eller till en extern enhet.

Regler och rutiner för informationsöverföring
Formella regler, rutiner och säkerhetsåtgärder ska vara införda för att skydda överföring av information genom användning av alla typer av kommunikationsmedel.

Överenskommelser om informationsöverföring
Säker överföring av verksamhetsinformation mellan organisationen och externa parter ska vara reglerad genom överenskommelser.

Elektronisk meddelandehantering
Information som hanteras genom elektronisk meddelandehantering (t.ex. e-post, sociala medier m.m.)ska ges lämpligt skydd.

Kapitel 10. Anskaffning, utveckling och underhåll av system

Detta kapitel beskriver vad som ska omfattas och beaktas vid anskaffning, utveckling, underhåll oav informationssystem.

10.1 Säkerhetskrav på informationssystem

Fokus: Att säkerställa att informationssäkerhet är en integrerad del av alla informationssystems hela livscykel.

Analys och specifikation av informationssäkerhetskrav
Inga informationssystem får anskaffas eller utvecklas utan att det har gjorts en analys av hur systemet förhåller sig till lagar, avtal och regler som styr kommunens verksamhet. Resultatet av analysen ska ligga till grund för informationssäkerhetskrav vid anskaffning och utveckling.

Säkerställande av programtjänster på publika nätverk
Information i programtjänster på publika nätverk ska skyddas från bedräglig aktivitet, avtalstvist samt obehörigt röjande och modifiering.

10.2 Säkerhet i utvecklings- och supportprocesser

Fokus: Att säkerställa att informationssäkerhet utformas och införs inom utvecklingscykeln för informationssystem.

Regler för säker utveckling
Regler för utveckling av informationssystem och tjänster ska upprättas och tillämpas.

Rutiner för hantering av systemändringar
Vid införande eller vid större ändringar av informationssystem och tjänster ska en formell process för förändringshantering följas. Processen ska omfatta test och verifiering samt riskanalys och specificeringav nödvändiga säkerhetsåtgärder.

Teknisk granskning av tillämpningar efter ändringar i driftsmiljö
När driftsmiljön ändras ska verksamhetskritiska tillämpningar granskas och testas för att säkerställa att det inte innebär negativ påverkan på verksamheten eller säkerheten.

Restriktioner för ändringar av programpaket
Ändringar av programpaket ska förhindras eller begränsas till nödvändiga ändringar och alla ändringar ska styras noggrant.

Principer för utveckling av säkra informationssystem
Riktlinjer för utveckling av säkra system ska upprättas, dokumenteras, underhållas och tillämpas vid alla införanden av informationssystem. Normalt sker ingen utveckling inom kommunen.

Säker utvecklingsmiljö
För systemutveckling ska organisationen upprätta och på lämpligt sätt skydda säkra utvecklingsmiljöer över systemets hela livscykel. Normalt sker ingen utveckling inom kommunen.

Outsourcad utveckling
Kommunen ska övervaka och styra outsourcad systemutveckling. Normalt sker ingen utveckling.

Säkerhetstestning
Säkerhetsfunktionalitet ska testas vid utveckling. Normalt sker ingen utveckling inom kommunen.

Acceptanstestning av system
Program för acceptanstester och relaterade kriterier ska fastställas för nya informationssystem, uppgraderingar och nya versioner.

10.3 Testdata

Fokus: Att säkerställa skyddet av data som används för tester

Skydd av testdata
Testdata ska väljas ut noggrant, skyddas och styras.

Kapitel 11. Leverantörsrelationer

11.1 Informationssäkerhet i leverantörsrelationer

Fokus: Detta kapitel beskriver vad som ska omfattas och beaktas i leverantörsrelationer för att säkerställa skydd av kommunens informationstillgångar.

Informationssäkerhetsregler för leverantörsrelationer
Informationssäkerhetskrav för att reducera riskerna förknippade med leverantörers åtkomst till organisationens tillgångar ska avtalas med leverantören och dokumenteras.

Hantering av säkerhet inom leverantörsavtal
Alla relevanta informationssäkerhetskrav ska avtalas med varje leverantör som kan tillgå, behandla, lagra och kommunicera information eller som tillhandahåller informationssystem och tjänster till kommunen.

Försörjningskedja för informations- och kommunikationsteknologi
Avtal med leverantörer ska innehålla krav på att hantera informationssäkerhetsriskerna förknippade med försörjningskedjan för informationssystem, produkter och tjänster baserade på informations- och kommunikationsteknologi.

Med försörjningskedjan avses samtliga aktörer som är delaktiga i framtagande och leverans av informationssystem, produkter och tjänster.

11.2 Hantering av leverantörers tjänsteleverans

Övervakning och granskning av leverantörstjänster
Organisationer ska regelbundet övervaka, granska och genomföra revision av sina leverantörers tjänsteleverans.

Ändringshantering av leverantörers tjänster
Ändringar av tillhandahållande av tjänster från leverantörer, med tillhörande regelverk och befintliga rutiner ska hanteras, med beaktande av informationens, systemens och processernas kritiska betydelse för verksamheten och riskerna ska omvärderas.

Kapitel 12. Hantering av informationssäkerhetsincidenter

12. 1 Hantering av informationssäkerhetsincidenter och förbättringar

Ansvar och rutiner
Det ska finnas processer som stödjer snabb, verkningsfull och korrekt hantering av informationssäkerhetsincidenter.

Rapportering av informationssäkerhetsincident
Informationssäkerhetshändelser ska rapporteras genom lämpliga rapporteringsvägar så snabbt som möjligt.

Rapportering av svagheter gällande informationssäkerhet
Anställda och leverantörer som använder organisationens informationssystem och tjänster ska göras skyldiga att notera och rapportera alla observerade eller misstänkta svagheter gällande informationssäkerhet i system eller tjänster.

Bedömning av och beslut om informationssäkerhetsincidenter
Händelser ska bedömas och beslut ska fattas om de ska klassas som informationssäkerhets-incidenter.

Hantering av informationssäkerhetsincidenter
Informationssäkerhetsincidenter ska hanteras i enlighet med dokumenterade rutiner.

Att lära av informationssäkerhetsincidenter
Kunskaper baserade på analyser av hanterade informationssäkerhetsincidenter ska användas för att minska sannolikheten eller påverkan av framtida incidenter.

Insamling av bevis
Kommunen ska fastställa och tillämpa rutiner för identifiering, insamling, kopiering och bevarande av information som kan tjäna som bevis. Normalt innebär det att följa direktiv från t.ex. polis.

Kapitel 13. Informationssäkerhetsaspekter avseende hantering av verksamhetens kontinuitet

13.1 Kontinuitet för informationssäkerhet
Fokus: Kontinuiteten för informationssäkerhet ska integreras i kommunens verksamheter.

Planering av kontinuitet för informationssäkerhet
Organisationen ska fastställa sina krav för informationssäkerhet och kontinuitet för styrning i svåra situationer, exempelvis under ett längre driftstopp, en kris eller en katastrof.

Införa kontinuitet för informationssäkerhet
Organisationen ska fastställa, dokumentera, införa och upprätthålla processer, rutiner och säkerhetsåtgärder för att säkerställa den nivå av kontinuitet för informationssäkerhet som krävs vid en svår situation.

Styra, granska och utvärdera kontinuitet för informationssäkerhet
Kommunen ska verifiera de fastställda och införda åtgärderna för kontinuitet av informationssäkerhetmed jämna mellanrum för att säkerställa att de är giltiga och verkningsfulla under störningar.

13.2 Redundans
Fokus: Att säkerställa tillgänglighet till information, informationssystem och tjänster.

Tillgänglighet till informationsbehandlingsresurser
Informationsbehandlingsresurser ska vid införande ha tillräcklig redundans för att uppfylla de krav på tillgänglighet som systemet och dess information ställer på verksamheten.

Kapitel 14. Efterlevnad

14.1 Efterlevnad av juridiska och avtalsmässiga krav

Fokus: Att undvika överträdelser av lagar, förordningar och/eller avtalsmässiga skyldigheter relaterade till informationssäkerhet och/eller eventuella säkerhetskrav.

Identifiering av tillämplig lagstiftning och avtalsmässkrav

Alla relevanta avtalskrav och organisationens tillvägagångssätt för att uppfylla dessa krav ska uttryckligen identifieras, dokumenteras och hållas uppdaterade för varje informationssystem och för organisationen.

Immateriella rättigheter

Lämpliga rutiner ska införas för att säkerställa efterlevnad av författningsenliga och avtalsmässiga krav relaterade till immateriella rättigheter och användning av upphovsskyddade programprodukter.

Skydd av dokumenterad information

Dokumenterad information ska skyddas från förlust, förstörelse, förfalskning, obehörig åtkomst och otillåten utgivning i enlighet med författningsenliga, avtalsmässiga och verksamhetsmässiga krav.

Skydd av personlig integritet och personuppgifter

I förekommande fall bör skydd av personlig integritet och personuppgifter säkerställas i enlighet med gällande författningar.

Reglering av kryptografiska säkerhetsåtgärder

Kryptografiska säkerhetsåtgärder ska användas i enlighet med gällande avtal och författningar.

14.2 Granskning av informationssäkerhet

Fokus: Att säkerställa att informationssäkerhet införs och drivs i enlighet med kommunens regler och rutiner.

Oberoende granskning av informationssäkerhet

Organisationens tillvägagångssätt för att hantera informationssäkerhet och dess införande (d.v.s. mål, säkerhetsåtgärder, regler, processer och rutiner för informationssäkerhet) ska med jämna mellanrum, eller när betydande förändringar sker, genomgå oberoende granskning.

Efterlevnad av säkerhetspolicy, regler och standarder

Högsta ledningen ska inom gällande ansvarsområden regelbundet granska efterlevnaden av informationssäkerhetspolicyn, gällande regler och riktlinjer, standarder och eventuella andra säkerhetskrav i förhållande till informationsbearbetning och rutiner.

Granskning av teknisk efterlevnad

Informationssystem ska granskas regelbundet avseende efterlevnad av organisationens informationssäkerhetspolicy, regler, riktlinjer och standarder.