Oskarshamns kommun

Styrande dokument

Riktlinje

Riktlinje för informationssäkerhet

Oskarshamns kommun

Riktlinje för informationssäkerhet

Ansvarig för dokumentet: Informationssäkerhetsansvarig
Omfattar: Alla verksamheter inom Oskarshamns kommun samt kommunala bolag
Informationsklass: Öppen
Publicering: Författningssamling
Beslutsinstans: Kommunstyrelsen
Fastställd: 2024-01-23
Gäller från och med: 2024-01-23
Giltighetstid: Tillsvidare
Ersätter: Riktlinjer för informationssäkerhet
Diarienummer: KS 2023/000945

Oskarshamns kommun

Innehåll

Riktlinje för informationssäkerhet **1**

1 SYFTE MED DETTA DOKUMENT OCH ÖVERGRIPANDE INFORMATION **10**

1.1 Beskrivning av informationssäkerhet 10

2 OMFATTNING **11**

2.1 Revision och ständig förbättring 11

3 TERMER OCH DEFINITIONER **12**

4 HÄNVISNINGAR **15**

4.1 Standarder och ramverk 15

4.2 Lagar och regelverk 15

5 POLICY **16**

5.1 Informationssäkerhetspolicy 16

6 ORGANISATION **17**

6.1 Roller och ansvar inom den politiska ledningen 17

6.1.1 Kommunfullmäktige 17

6.1.2 Kommunstyrelsen 17

6.1.3 Nämnd eller bolagsstyrelse 17

6.2 Roller och ansvar i verksamheten 17

6.2.1 Ansvar beskrivet i informationssäkerhetspolicy 17

6.3 Övriga roller 19

7 PERSONALSÄKERHET **20**

7.1 Före anställning 20

7.1.1 Bakgrundskontroll 20

7.1.2 Anställningsvillkor 20

7.2 Under anställning 20

7.2.1 Ledningens ansvar 20

7.2.2 Medvetenhet, utbildning och fortbildning i informationssäkerhet 21

7.2.3 Disciplinära åtgärder 21

7.3 Avslut eller ändring av anställning 21

7.3.1 Avslut eller ändring av anställds ansvar 21

8 HANTERING AV TILLGÅNGAR **22**

8.1 Ansvar för tillgångar 22

8.1.1 Inventering av tillgångar 22

8.1.2 Ägarskap av tillgångar 22

8.1.3 Tillåten användning av tillgångar 22

8.1.4 Återlämnande av tillgångar 22

8.2 Informationsklassning 23

8.2.1 Klassning av information 23

8.2.2 Märkning av information och tillgångar 23

8.2.3 Hantering av tillgångar ... 24
8.3 Hantering av informationsrisk ... 24
8.3.1 Riskanalys ... 24
8.3.2 Riskbehandling ... 25
8.3.3 Incidenthantering ... 25
8.4 Hantering av lagringsmedia ... 25
8.4.1 Hantering av flyttbara lagringsmedia ... 25
8.4.2 Avveckling av lagringsmedia ... 25
8.4.3 Transport av fysiska lagringsmedia ... 25
8.5 Hantering pappersbaserad information ... 26
8.5.1 Märkning ... 26
8.5.2 Förvaring ... 26
8.5.3 Avveckling ... 26
8.6 Mobil utrustning och distansarbete ... 27
8.6.1 Regler för mobil utrustning ... 27
8.6.2 Distansarbete ... 27
8.6.3 Användning av privat utrustning vid hantering av kommunens information ... 27
9 STYRNING AV ÅTKOMST ... 28
9.1 Verksamhetskrav för styrning av åtkomst ... 28
9.1.1 Regler för styrning av åtkomst ... 28
9.1.2 Tillgång till nätverk och nätverkstjänster ... 28
9.2 Hantering av användaråtkomst ... 28
9.2.1 Registrering och avregistrering av användare ... 29
9.2.2 Tilldelning av behörigheter ... 29
9.2.3 Hantering av privilegierade åtkomsträttigheter (”Admin”) ... 29
9.2.4 Hantering av användares inloggningsuppgifter ... 29
9.2.5 Granskning av användares behörigheter och åtkomsträttigheter ... 29
9.2.6 Borttagning eller justering av behörigheter och åtkomsträttigheter ... 29
9.3 Användaransvar ... 30
9.3.1 Användning av inloggningsuppgifter ... 30
9.4 Styrning av åtkomst till information, informationssystem och tjänster ... 30
9.4.1 Begränsning av åtkomst till information ... 30
9.4.2 Säkra in- och utloggningsrutiner ... 30
9.4.3 Lösenordshantering ... 31
9.4.4 Systemsäkerhet ... 31
10 KRYPTERING ... 32
10.1 Kryptografiska säkerhetsåtgärder ... 32
10.1.1 Regler för användning av kryptering ... 32
10.1.2 Nyckelhantering ... 32
11 FYSISK OCH MILJÖRELATERAD SÄKERHET ... 33

11.1 Säkra områden ... 33
11.1.1 Fysiska säkerhetsavgränsningar ... 33
11.1.2 Fysiska tillträdesbegränsningar ... 33
11.1.3 Säkerställande av kontor, rum och anläggningar ... 33
11.1.4 Skydd mot yttre och miljörelaterade hot ... 33
11.1.5 Arbeta i säkra utrymmen ... 33
11.2 Utrustning ... 34
11.2.1 Placering och skydd av utrustning ... 34
11.2.2 Tekniska försörjningssystem ... 34
11.2.3 Kablagesäkerhet ... 34
11.2.4 Underhåll av utrustning ... 34
11.2.5 Utförsel av tillgångar ... 34
11.2.6 Säkerhet för utrustning och tillgångar utanför organisationen ... 34
11.2.7 Säker kassering eller återanvändning av utrustning ... 34
11.2.8 Obevakad utrustning som hanteras av användare ... 35
12 DRIFTSÄKERHET ... 36
12.1 Driftrutiner och ansvar ... 36
12.1.1 Dokumenterade driftsrutiner ... 36
12.1.2 Ändringshantering ... 36
12.1.3 Kapacitetshantering ... 36
12.1.4 Separation av utvecklings-, test- och driftmiljöer ... 36
12.2 Skydd mot skadlig kod ... 37
12.2.1 Säkerhetsåtgärder mot skadlig kod ... 37
12.3 Säkerhetskopiering ... 37
12.3.1 Säkerhetskopiering av information ... 37
12.4 Loggning och övervakning ... 37
12.4.1 Loggning av händelser ... 37
12.4.2 Skydd av logginformation ... 38
12.4.3 Administratörs- och operatörsloggar ... 38
12.4.4 Synkronisering av tid ... 38
12.5 Styrning av informationssystem ... 38
12.5.1 Installation av program ... 38
12.6 Hantering av tekniska sårbarheter ... 38
12.6.1 Hantering av tekniska sårbarheter ... 38
12.6.2 Användares restriktioner för installation av program ... 38
12.7 Överväganden gällande revision av informationssystem ... 39
12.7.1 Tekniska revisionskontroller för informationssystem ... 39
13 KOMMUNIKATIONSSÄKERHET ... 40
13.1 Hantering av nätverkssäkerhet ... 40
13.1.1 Säkerhetsåtgärder för nätverk ... 40

13.1.2 Säkerhet hos nätverkstjänster ... 40
13.1.3 Separation av nätverk ... 40
13.2 INFORMATIONSÖVERFÖRING ... 40
13.2.1 Regler och rutiner för informationsöverföring ... 40
13.2.2 Överenskommelser om informationsöverföring ... 40
13.2.3 Elektronisk meddelandehantering ... 41
14 DATASKYDD ... 42
14.1 Hantering av personuppgifter ... 42
14.1.1 Personuppgiftansvar ... 42
14.1.2 Behandling av personuppgifter ... 42
14.1.3 Säkerhet inom dataskydd ... 43
14.1.4 Vid användande av personuppgiftsbiträde ... 43
14.1.5 Särskilt skydd av personer med skyddade personuppgifter ... 44
15 SÄKER LIVSCYKEL HOS INFORMATIONSSYSTEM ... 45
15.1 Säkerhetskrav på informationssystem ... 45
15.1.1 Analys och specifikation av informationssäkerhetskrav ... 45
15.1.2 Säkerhetskrav på publika tjänster ... 45
15.2 Säkerhet i utvecklings- och supportprocesser ... 45
15.2.1 Regler för säker utveckling ... 45
15.2.2 Rutiner för hantering av ändringar i informationssystem och tjänster ... 46
15.2.3 Rutiner för hantering av ändringar i driftsmiljö ... 46
15.2.4 Restriktioner för ändringar av programpaket ... 46
15.2.5 Principer för utveckling av säkra informationssystem ... 46
15.2.6 Säker utvecklingsmiljö ... 46
15.2.7 Outsourcad utveckling ... 46
15.2.8 Systemtest med inriktning säkerhet ... 46
15.2.9 Acceptanstestning av informationssystem och tjänster ... 46
15.3 Testdata ... 47
15.3.1 Skydd av testdata ... 47
16 LEVERANTÖRSRELATIONER ... 48
16.1 Informationssäkerhet i leverantörsrelationer ... 48
16.1.1 Informationssäkerhetsregler för leverantörsrelationer ... 48
16.1.2 Hantering av säkerhet inom leverantörsavtal ... 48
16.1.3 Försörjningskedja för informations- och kommunikationsteknologi ... 48
16.2 Hantering av leverantörers tjänsteleverans ... 48
16.2.1 Övervakning och granskning av leverantörstjänster ... 48
16.2.2 Ändringshantering av leverantörers tjänster ... 49
17 HANTERING AV INFORMATIONSSÄKERHETSINCIDENTER ... 50
17.1 Hantering av incidenter och förbättringar ... 50
17.1.1 Ansvar och rutiner ... 50

17.1.2 Rapportering av informationssäkerhetsincident 50
17.1.3 Rapportering av svagheter gällande informationssäkerhet 50
17.1.4 Bedömning av och beslut om informationssäkerhetsincidenter 50
17.1.5 Hantering av informationssäkerhetsincidenter 50
17.1.6 Att lära av informationssäkerhetsincidenter 50
17.1.7 Insamling av bevis 50
18 VERKSAMHETENS KONTINUITET 51
18.1 Kontinuitet för informationssäkerhet 51
18.1.1 Planering av kontinuitet för informationssäkerhet 51
18.1.2 Införa kontinuitet för informationssäkerhet 51
18.1.3 Styra, granska och utvärdera kontinuitet för informationssäkerhet 51
18.2 Redundans 51
18.2.1 Tillgänglighet för informationssystem 51
19 EFTERLEVNAD 52
19.1 Efterlevnad av juridiska och avtalsmässiga krav 52
19.1.1 Identifiering av gällande lagstiftning och avtalsmässiga krav 52
19.1.2 Immateriella rättigheter 52
19.1.3 Skydd av dokumenterad information 52
19.1.4 Reglering av kryptografiska säkerhetsåtgärder 52
19.2 Mätning och granskning av informationssäkerhet 52
19.2.1 Löpande mätning av säkerhet och säkerhetsincidenter 52
19.2.2 Extern granskning 53
19.2.3 Intern granskning 53
19.2.4 Granskning av teknisk efterlevnad 53

Oskarshamns kommun

Läsanvisning

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

Kapitel 1. Beskriver riktlinjens syfte.

Kapitel 2. Beskriver riktlinjens omfattning.

Kapitel 3. Beskriver termer och definitioner som förekommer i riktlinjen.

Kapitel 4. Hänvisar till standarder, lagar och förordningar för informationssäkerhet.

Kapitel 5. Beskriver relationen policy, riktlinjer och instruktioner samt uttrycker ledningens stöd för informationssäkerhetsarbetet.

Kapitel 6. Beskriver roller och ansvar uppdelat på politikens respektive verksamhetens ansvar. För att uppnå och behålla en god informationssäkerhet är det viktigt att roller och ansvar tydliggörs. I detta kapitel beskrivs vilken roll som ansvarar för vad.

Kapitel 7. Beskriver personalens och andra kategoriers ansvar för informationssäkerheten. Alla som arbetar i eller för kommunens verksamhet behöver förstå sitt ansvar för och bidra till att hantera och skydda kommunens tillgångar.

Kapitel 8. Beskriver hur vi ska hantera kommunens informationstillgångar. Sekretessbelagda handlingar, patient- och brukaruppgifter är exempel på känslig information som vi måste hantera på särskilt sätt. Genom att placera klassificera informationen vet vi vilka tillgångar som kräver mer skydd än andra tillgångar.

Kapitel 9. Hur ska vi förhindra att obehöriga får åtkomst till kommunens informationssystem, IT-tjänster och infrastruktur? Riktlinjen beskriver hur åtkomst till information ska styras så att endast behöriga användare kommer åt informationen.

Kapitel 10. Beskriver hur när kryptering som skyddsåtgärd kan vara aktuell och regler för detta. Syftar till att skydda information från insyn och förvanskning.

Kapitel 11. Beskriver hur IT-systemen och informationstillgångarna skyddas. Det kan handla om hur vi säkrar tillträdet till känsliga utrymmen, hur skalskydden ska dimensioneras samt krav på brandskydd.

Kapitel 12. Beskriver hur vi uppnår en god driftsäkerhet. För att undvika störningar och driftstopp i kommunens IT-miljö behövs en god förvaltning med noggranna rutiner för hur till exempel driftsättning, kopiering och loggning.

Kapitel 13. Beskriver specifikt hanteringen av personuppgifter.

Kapitel 14. Beskriver de krav som finns för att skydda nätverket mot t.ex. avlyssning, intrång samt avbrott.

Kapitel 15. Beskriver säkerhetskrav vid utveckling, säkerställer att informationssäkerhet finns med från början. För de system som kommunen inte utvecklar själva, ska kraven ställas på leverantören.

Kapitel 16. Beskriver krav på leverantörer.

Kapitel 17. Hantering av incidenter som rör informationssäkerhet. När en allvarlig incident inträffar är det viktigt att vi agerar snabbt för att begränsa eller avvärja konsekvenserna av den. Störningar kan ha flera orsaker och kan snabbt komma att påverka många delar av kommunens verksamhet. I detta kapitel behandlas hur vi hanterar sådana händelser.

Kapitel 18. Kontinuitetsplanering innebär att verksamheten ska kunna pågå även när tillgången till IT-stödet uteblir. Därför är det viktigt att planera för hur verksamheten ska fungera om något händer. Hör finns riktlinjerna för hur vi gör det och planerar för kontinuitet.

Kapitel 19. Om efterlevnad av legala och avtalsmässiga krav. Mätning av säkerhet med avseende på uppnådd effekt och utfört arbete.

1 SYFTE MED DETTA DOKUMENT OCH ÖVERGRIPANDE INFORMATION

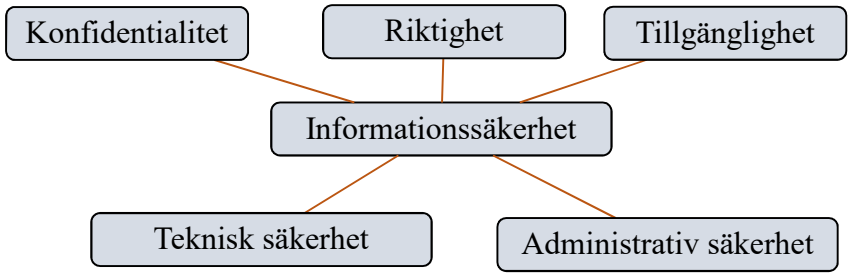
Dessa riktlinjer för informationssäkerhet syftar till att beskriva ”Vad” som ska göras för att uppfylla ledningens viljeyttring.

Dokumentet utgör kommunens och dess helägda bolags riktlinjer för informationssäkerhet och ingår i dess ledningssystem för informationssäkerhet. Riktlinjerna är underställd den av kommunfullmäktige beslutade informationssäkerhetspolicyn.

1.1 Beskrivning av informationssäkerhet

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 av både 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.

2 OMFATTNING

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

Samtliga anställda, extern personal, politiker som aktivt arbetar i verksamheten omfattas av policyn och dess tillhörande riktlinjer och instruktioner. Övriga, t.ex. politiker och elever som ges tillgång till kommunens IT-nätverk skall också omfattas.

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

2.1 Revision och ständig förbättring

Dokumentet ska revideras vid större förändringar, dock minst en gång per mandatperiod

Oskarshamns kommun

3 TERMER OCH DEFINITIONER

För användningen av dessa riktlinjer gäller följande termer och definitioner

Autentisering;
Kontroll av uppgiven identitet.

Behandling av personuppgifter;
Varje åtgärd eller serie av åtgärder som någon vidtar med personuppgifter, vare sig det görs på automatiserad väg eller inte.

Behörighet;
Tilldelad åtkomsträttighet i IT-system.

Hot;
Möjlig oönskad händelse med negativa konsekvenser för verksamheten.

Information;
Ett vitt begrepp som inkluderar allt från kunskap som enskilda medarbetare besitter till information lagrad i IT-system.

Informationstillgång;
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 samt all form av film, ljud och bild.

Informationsrisk;
Risk där konsekvensen uttrycks i konfidentialitet, riktighet eller tillgänglighet.

Informationssäkerhet;
Bevarande av konfidentialitet, riktighet och tillgänglighet hos information.
Härutöver kan begreppet även innefatta till exempel spårbarhet, autenticitet, oavvislighet och tillförlitlighet.

Informationssäkerhetsincident;
En eller flera händelser som kan tänkas få allvarliga konsekvenser för verksamheten och hota informationssäkerheten (till exempel brott mot sekretess, integritetsförlust, driftavbrott eller brist på tillgång till information).

Informationssäkerhetspolicy; Övergripande avsikt och viljeinriktning formellt uttryckt av en organisations ledning. Anger mål och inriktning för samt styr informationssäkerhetsarbetet inom organisationen.

IT-system;
Informationsbehandlingssystem som med informationsteknik hanterar och utbyter

information med omgivningen. I begreppet IT-system innefattas även kommunikations-utrustning, datorer, servrar, skrivare och övrig teknisk utrustning som ansluts till kommunens kommunikationsnätverk.

Konfidentialitet;
Egenskap att information inte görs tillgänglig eller avslöjas för obehöriga personer, enheter eller processer.

Känsliga personuppgifter;
Uppgifter som avslöjar etniskt ursprung, politiska åsikter, religiös eller filosofisk 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 teknisk enhet.

OT-system;
Operativ Teknik/Operational Technology, tekniska system som SCADA, drift-, styr-, larm- och passersystem.

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 personuppgifter, även om inga namn nämns. Krypterade uppgifter och olika slag av elektroniska identiteter är också personuppgifter om de direkt eller indirekt kan kopplas till fysiska personer som är i livet.

Riktighet;
skydd mot oönskad förändring.

Risk;
Produkten av sannolikheten och konsekvensen för att ett givet hot realiseras.

Riskanalys;
Metodisk aktivitet som identifierar, beskriver och kvantifierar risk inom ett givet område, t.ex. ett system.

Sammanhållen journalföring;
Ett elektroniskt system, som gör det möjligt för en vårdgivare att ge eller få direktåtkomst till personuppgifter.

Samtycke;
Varje slag av otvetydig viljeyttring genom vilken den registrerade godtar att personuppgifter som rör honom eller henne behandlas.

SCADA;
Supervisory Control and Data Acquisition, så kallade digitala kontrollsystem. Datorbaserade

system för styrning, reglering och övervakning av fysiska processer som till exempel el-, gas- och vattenförsörjning samt spårbunden trafik.

SITHS-kort;
Tjänstekort med elektronisk ID som används för autentisering vid inloggning till IT-system, främst vårdrelaterade.

Skadlig kod;
Otillåten programkod som syftar till för att ändra, röja, förstöra, störa eller avlyssna ett datanät, funktioner eller uppgifter i IT-system.

Skyddsåtgärd;
Handling, procedur eller tekniskt arrangemang som genom att minska sårbarheten möter identifierade hot.

Spårbarhet;
Entydig härledning av utförda aktiviteter till en identifierad användare eller process.

Stark autentisering;
Autentisering som innebär att identiteten kontrolleras på minst två sätt.

Sårbarhet;
Brist i skyddet av en tillgång eller en grupp av tillgångar exponerad för hot.

Tillgång;
Något som har värde för en organisation. Med informationstillgångar menas informationen i sig och de resurser som används för att hantera den, till exempel programvaror, tjänster och fysiska tillgångar.

Tillgänglighet;
Egenskap att vara tillgänglig och användbar på begäran av en behörig aktör

Oskarshamns kommun

4 HÄNVISNINGAR

4.1 Standarder och ramverk

De interna styrdokumenten baseras på Svensk standard för informationssäkerhet.

- SS-ISO/IEC 27001:2014 (Krav på informationssäkerhet)
- SS-ISO/IEC 27002:2014 (Riktlinjer för informationssäkerhet)

4.2 Lagar och regelverk

Kraven på informationssäkerheten 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. Det finns myndigheter och organisationer som ger särskilt stöd genom att upprätta förteckningar om lagar och regelverk

5 POLICY

5.1 Informationssäkerhetspolicy

Målet med informationssäkerhetspolicyn är att redovisa ledningens viljeinriktning och stöd för informationssäkerhetsarbetet. Informationssäkerhetspolicyn fastställs av kommunfullmäktige.

I policyn delegerar även kommunfullmäktige följande;

- vad och varför något skall åstadkommas
- vem som ansvarar för att detta uppnås
- hur detta skall följas upp

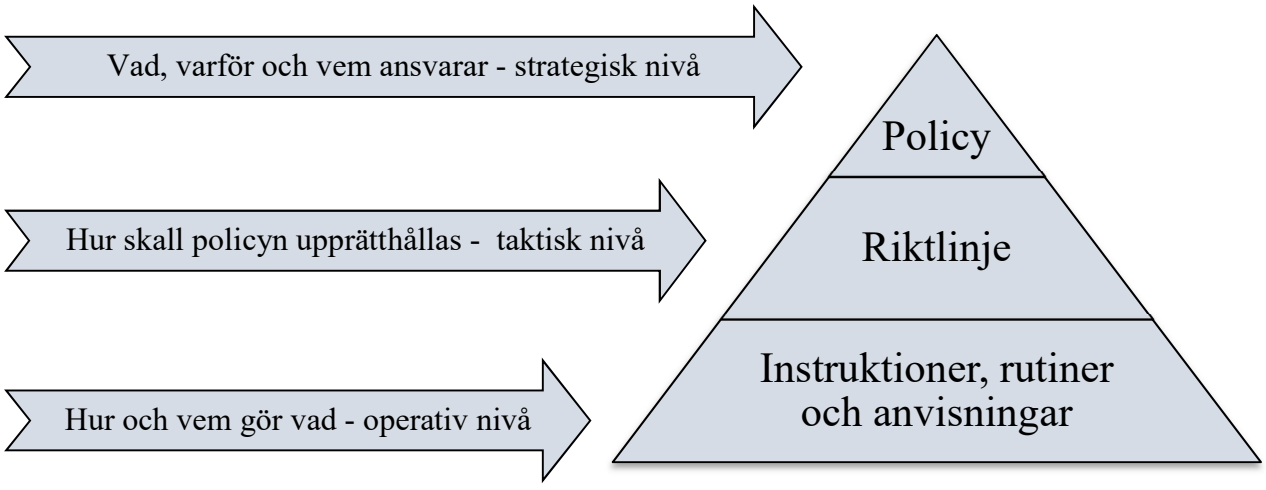
Riktlinjer för informationssäkerhet är underställd informationssäkerhetspolicyn och fastställs av kommunstyrelsen.

- Riktlinjerna beskriver hur ansvar och mål upprätthålls
- I riktlinjerna beskrivs organisationen för informationssäkerhetsarbetet

Beslutad policy och riktlinjer utgör tillsammans med anvisningar, rutiner och instruktioner styrdokument för informationssäkerhet.

Anvisningar, rutiner och instruktioner fastställs på verksamhetsnivå.

Verksamhetens ordinarie processer skall inkludera informationssäkerhet.



6 ORGANISATION

Syfte: Att upprätta en organisation för att initiera och styra införandet och förvaltningen av informationssäkerhetsarbetet i kommunen och dess helägda bolag.

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

6.1 Roller och ansvar inom den politiska ledningen

Den politiska ledningen har det övergripande ansvaret för informationssäkerhet.

Kommunfullmäktige, kommunstyrelsen och respektive facknämnders/bolagsstyrelser ansvar för informationssäkerhetsarbetet beskrivs kortfattat nedan.

6.1.1 Kommunfullmäktige

Kommunfullmäktige fastställer en policy för informationssäkerhet, vilken uttrycker viljeinriktningen för kommunens arbete med informationssäkerhet.

6.1.2 Kommunstyrelsen

Kommunstyrelsen fastställer riktlinjer för informationssäkerhet och har det yttersta ansvaret för kommunens informationssäkerhetsarbete samt kommunstyrelsens verksamheter. Kommunstyrelsen utser Dataskyddsombud för dess verksamhet och är ytterst personuppgiftsansvarig för sina verksamheter.

6.1.3 Nämnd eller bolagsstyrelse

De kommunala nämnderna/bolagsstyrelsen har det praktiska ansvaret för informationssäkerhetsarbetet inom sina respektive verksamheter/myndigheter. Nämnden/bolagsstyrelsen är personuppgiftsansvarig och utser Dataskyddsombud för dess verksamhet.

6.2 Roller och ansvar i verksamheten

6.2.1 Ansvar beskrivet i informationssäkerhetspolicy

6.2.1.1 Kommunchef/-direktör, bolagschef eller förvaltningschef

Ansvarar för att utse objektägare och informationsägare.

6.2.1.2 Varje chef

Varje chef ansvarar för att det finns rutiner som säkerställer en god efterlevnad av kommunens regelverk för informationssäkerhet.

6.2.1.3 Informationssäkerhetssamordnaren

Har det övergripande och strategiska ansvaret att leda, utveckla och samordna informations-säkerhetsarbetet samt föreskriva de metoder som skall använda för riskanalys och informationsklassning.

6.2.1.4 Informationsägare

Har det övergripande och yttersta ansvaret för den informationsmängd som delegerats dem. Informationsägarna avgör vilken information som får hanteras, hur den hanteras och av vem. Informationsägarna har också ansvar för att informationsklassning och att riskanalyser genomförs för den informationsmängd som de ansvarar för.

6.2.1.5 Objektägare

Har ett övergripande ansvar för förvaltningsobjektet och för att det uppfyller verksamhetens behov och lagkrav. System som ingår i förvaltningsobjektet ska uppfylla informationssäkerhetskraven i förhållande till verksamhetens behov, legala krav och säkerhetskrav. Systemens informationsmängder ska klassificeras.

6.2.1.6 Objektledare

Har det funktionella helhetsansvaret för alla system i förvaltningsobjektet. Objektledaren ser till att verksamheten stöds genom att funktionalitet upprätthålls och utvecklas. Objektledaren planerar och delegerar aktiviteter inom förvaltningsobjektet.

I riktlinjen ”Samverkansmodell för objektförvaltning” beskrivs rollerna i detalj, samt övriga stödjande roller som krävs.

6.2.1.7 Dataskyddsombud

Personuppgiftsansvarig är den som bestämmer varför och hur personuppgifter ska behandlas. Oskarshamns kommuns nämnder är personuppgiftsansvariga för sina respektive behandlingar av personuppgifter. Varje personuppgiftsansvarig har skyldighet att tillsätta ett Dataskyddsombud enligt Dataskyddsförordningen, med sakkunskap om lagstiftning och praxis om dataskydd. Rollen skall vara självständig, rådgivande och övervakande i att kommunen följer reglerna i Dataskyddsförordningen. I Oskarshamns Kommun anlitar vi Sydarkivera som Dataskyddsombud.

6.2.1.8 Digitaliseringschef

Har det operativa ansvaret för att uppfylla gällande krav på informationssäkerhet som ställs på den tekniska IT-infrastrukturen.

6.3 Övriga roller

Kommunens/bolagens verksamhetsledning bestående av ledande tjänstepersoner har det organisatoriska ansvaret för arbetet med informationssäkerhet. Kommundirektören, bolagschef och förvaltningscheferna har särskilt ansvar för organisation, ledning och styrning av informationssäkerhetsarbetet.

Alla som hanterar informationstillgångar har ett ansvar för att informationssäkerheten upprätthålls.

Oskarshamns kommun

7 PERSONALSÄKERHET

Detta kapitel beskriver vad som ska omfattas och beaktas i samband med rekrytering, anställning och avslutande av anställning.

Syfte: Att säkerställa att alla anställda och andra berörda förstår sitt ansvar och är lämpliga för de roller som de är tilltänkta för. Exempel på andra berörda roller är elever, politiker, inhyrd personal, tjänsteköp och leverantörer.

7.1 Före anställning

7.1.1 Bakgrundskontroll

Bakgrundskontroll på alla sökande för anställning ska utföras i enlighet med relevanta författningar, etiska krav och i proportion till verksamhetskraven, klassificeringen av information som de ges behörighet till och de upplevda riskerna. Exempel på bakgrundskontroll är utdrag ur belastningsregistret för till exempel förskollärare.

7.1.2 Anställningsvillkor

Verksamheterna ska i anställnings- eller arbetsvillkor inkludera ett uttalande om den anställdes ansvar för informationssäkerhet.

Samtliga medarbetare ska göras medvetna om sina skyldigheter enligt anställnings- eller annat tillämpligt avtal samt om gällande regler för informationssäkerhet och sekretess.

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

7.2 Under anställning

Syfte: Att säkerställa att anställda och andra berörda är medvetna om och uppfyller sitt ansvar för informationssäkerhet.

7.2.1 Ledningens ansvar

Varje chef ansvarar för att det finns rutiner som säkerställer att underställda kan efterleva kommunens regelverk för informationssäkerhet.

7.2.2 Medvetenhet, utbildning och fortbildning i informationssäkerhet

Kommunens målsättning är att en god säkerhetskultur ska genomsyra kommunen. Med detta menas inte bara att medarbetarna har god kunskap om vilka säkerhetsregler som gäller utan att de också använder gott omdöme och kritiskt ifrågasätter händelser som kan påverka säkerheten.

Samtliga anställda inom kommunen ska få den utbildning i informationssäkerhet som krävs för att de ska kunna utföra sina arbetsuppgifter och för att säkerställa målen för informationssäkerheten. Utbildningens omfattning ska vara anpassad till det ansvar och de befogenheter som gäller för befattningen.

7.2.3 Disciplinära åtgärder

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

7.3 Avslut eller ändring av anställning

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

7.3.1 Avslut eller ändring av anställds ansvar

Det ska finnas en rutin som hanterar när medarbetare (anställda, praktikanter och inhyrda konsulter) slutar sin anställning eller uppdrag inom kommunen. Ansvarsuppgifter ska avlämnas och åtkomsträttigheter upphöra vid anställningens eller uppdragets slut.

Oskarshamns kommun

8 HANTERING AV TILLGÅNGAR

Med tillgång avses här tillgångar som är relaterade till information och informationssystem.

8.1 Ansvar för tillgångar

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

Ansvaret för informationstillgångar utgår från beslutade ägarroller

8.1.1 Inventering av tillgångar

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

Inventera och kartlägg verksamhetens samtliga fysiska och virtuella enheter, on-prem eller i molnet.

All programvara ska inventeras.

8.1.2 Ägarskap av tillgångar

Tillgångar i förteckningen ska kopplas till en ägare.

8.1.3 Tillåten användning av tillgångar

Regler för tillåten användning av tillgångar ska identifieras, dokumenteras och införas.

Målgruppen för dessa riktlinjer ska göras medvetna om de krav på informationssäkerhet som gäller för tillgångarna.

Otillåten programvara ska tas bort. Programvara som krävs för verksamhet kan ges tillfälligt godkännande av informationssäkerhetsansvarig.

8.1.4 Återlämnande av tillgångar

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

Information som lagras och hanteras tillhör kommunen och ska återlämnas, t.ex. information i telefon, USB och andra externa lagringsmedier liksom information i skriven form på papper.

Oskarshamns kommun

8.2 Informationsklassning

Syfte: Att säkerställa att information får en lämplig skyddsnivå i överensstämmelse med dess betydelse för kommunen samt enligt gällande lagar och föreskrifter.

8.2.1 Klassning av information

Information ska klassas utifrån rättsliga krav, informationens värde för verksamheten och den enskilde. Informationsägaren ansvarar för att informationsklassning genomförs. Informationsklassningen ska revideras om förutsättningarna ändras. Nya förutsättningar kan t.ex. vara nya eller uppdaterade lagar och förordningar, systemets hantering av information eller nytt ändamål för systemet. Metoden för klassningen kan skiljas åt beroende på ifall det är ett enskilt dokument eller ett helt IT-system som ska klassas.

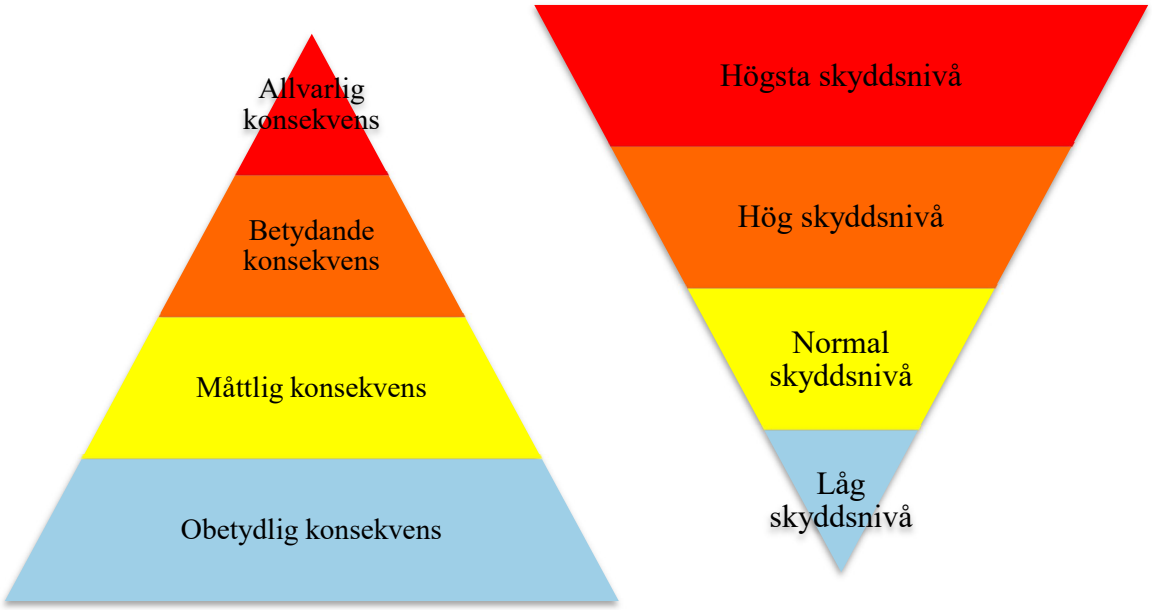
8.2.2 Märkning av information och tillgångar

En lämplig uppsättning rutiner för märkning av information ska utvecklas och införas i enlighet med den modell för informationsklassning som antagits.
Upprätta och underhåll riktlinjer för ett övergripande dataklassificeringssystem för företaget. Använd etiketter som "Hemlig", "Intern" och "Öppen" och klassificera data enligt dessa etiketter.

8.2.3 Hantering av tillgångar

En lämplig uppsättning rutiner för hantering av tillgångar ska utvecklas och införas i enlighet med den modell för informationsklassning som antagits.

Konkret så innebär det att information med hög klassning ska motsvaras av hög säkerhetsåtgärd och information med låg klassning motsvaras av låg säkerhetsåtgärd. Se nedanstående bild som illustrerar detta förhållande.



Upprätta en process för säker konfiguration. Processen gäller för både hårdvarutillgångar och programvara.

8.3 Hantering av informationsrisk

Syfte: Att möjliggöra ett effektivt skydd för tillgångar genom att upprätthålla en aktuell dokumenterad bild av möjliga, oönskade händelser.

8.3.1 Riskanalys

Informationsägaren ansvarar för att regelbundet genomföra och dokumentera analys av informationsrisk för sina tillgångar. Analysen ska avse händelser med konsekvens för såväl konfidentialitet, riktighet, tillgänglighet samt spårbarhet. Risker ska beskrivas på ett sätt som kan förstås av lekmän.

8.3.2 Riskbehandling

Risk som inte kan undvikas, överföras eller accepteras måste minskas så att antingen sannolikheten eller konsekvensen reduceras till nivåer som gör risken tolerabel. Det är informationsägarens ansvar att kravställa på teknikleverantörer och mänskliga aktörer att utforma och tillämpa de skydd som behövs för att minska risken som avsett.

8.3.3 Incidenthantering

Ibland inträffar oväntade och oönskade händelser som får (eller skulle kunnat få) konsekvens för tillgångar i termer av konfidentialitet, riktighet, tillgänglighet.

Se vidare i ”Rutin för incidenthantering”.

Organisationen ska utnyttja dessa händelser till att lära av det inträffade och förbättra hanteringen av sina tillgångar. Det är informationsägarens ansvar att uppdatera riskanalysen i ljuset av inträffade incidenter.

8.4 Hantering av lagringsmedia

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

8.4.1 Hantering av flyttbara lagringsmedia

Rutiner ska införas för hantering av flyttbara lagringsmedia i enlighet med den modell för informationsklassning som antagits. Användning av flyttbara lagringsmedia skall undvikas. Kryptera data på flyttbara medier.

Exempel på flyttbar lagringsmedia är USB-minnen, externa hårddiskar, minneskort och kamera.

8.4.2 Avveckling av lagringsmedia

Lagringsmedia ska avvecklas när det inte längre behövs i enlighet med den modell för informationsklassning som antagits. Formella rutiner skall fastställas av informationsägare.

8.4.3 Transport av fysiska lagringsmedia

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

Oskarshamns kommun

8.5 Hantering pappersbaserad information

Syfte: Att säkerställa säkerheten vid hantering och användning av pappersbaserad information.

8.5.1 Märkning

Handläggaren ansvarar för att ursprunget till pappersbaserad informationen kan härledas. Om informationen är pappersbaserad och blivit registrerad i dokument- och ärendehanteringssystem (eller annat verksamhetssystem med registreringsmöjlighet) ska papperet vara märkt med registreringsnummer/diarienummer.

Om den pappersbaserade informationen är sekretessbelagd ska handläggaren tillse att den är diarieförd (undantag finns). I dessa fall skall handlingen stämplas med sekretesstämpel. Observera att stämpel innebär att en sekretessprövning behöver göras.

8.5.2 Förvaring

Arbetsmaterial kring pågående ärenden med personuppgifter eller sekretessbelagd eller annan känslig information ska förvaras i låsbara utrymmen.

8.5.3 Avveckling

För att förstöring av pappershandlingar skall kunna ske (gäller all information) måste en informationshanteringsplan vara beslutad av ansvarig nämnd/styrelse.

Gallring ska utföras till sekretesstunnor eller dokumentförstörare, placerade innanför lokalens skalskydd.

Sekretesstunnor skall tömmas regelbundet av behörig leverantör, om möjligt säkerhetsklassad.

Dokumentförstörare ska strimla papper både horisontellt och vertikalt, för att informationen inte ska kunna återskapas utan stor ansträngning.

Oskarshamns kommun

8.6 Mobil utrustning och distansarbete

Syfte: Att säkerställa säkerheten vid distansarbete och användning av mobil utrustning.

8.6.1 Regler för mobil utrustning

Med mobil utrustning räknas mobiltelefoner, bärbara datorer, surfplattor och liknande.

Regler och instruktioner för hantering av mobil utrustning ska finnas baserat på informationsklassning och riskbedömning.

Vid användning av mobil utrustning ska särskild försiktighet iakttas för att säkerställa att verksamhetsinformation inte äventyras.

8.6.2 Distansarbete

Distansarbete avser alla former av arbete utanför kommunens lokaler och skalskydd.

Information som nås, bearbetas eller lagras på distansarbetsplatser ska skyddas enligt beslutade säkerhetsnivåer på samma sätt som om arbetet utfördes i kommunens lokaler.

Kommunen ansvar inte för förbindelse eller kapacitet vid distansarbete.

8.6.3 Användning av privat utrustning vid hantering av kommunens information

Privat utrustning skall inte användas för hantering av kommunens information i tjänsten.

Webbtjänster som är publikt tillgängliga externt får nyttjas även från privata enheter.

9 STYRNING AV ÅTKOMST

Åtkomst till information, informationssystem och tjänster ska begränsas i enlighet med informationsägares reglering genom att:

- säkerställa behörig åtkomst,
- förhindra obehörig åtkomst,
- göra användare ansvariga för att skydda sina inloggningsuppgifter som till exempel sitt lösenord, PIN-kod eller SITHS-kort

9.1 Verksamhetskrav för styrning av åtkomst

Syfte: Att säkerställa korrekt åtkomst till information, informationssystem och tjänster.

9.1.1 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. Åtkomstkontroller ska motsvara informationens klassificering.

Reglerna ska dokumenteras och vara möjliga att följa upp.

Centralisera åtkomstkontroll för alla företagstillgångar genom en katalogtjänst eller SSO-leverantör, där det stöds.

9.1.2 Tillgång till nätverk och nätverkstjänster

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

9.2 Hantering av användaråtkomst

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

Upprätta och underhåll ett inventarieregister av verksamhetens samtliga autentisering och behörighetssystem, inklusive de som finns på plats eller hos en fjärrtjänstleverantör.

9.2.1 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.

9.2.2 Tilldelning av behörigheter

En formell process för tilldelning av behörigheter ska finnas.

Tillgång till alla informationssystem ska styras med hjälp av åtkomstkontroll.

Externt exponerade applikationer skall ha flerfaktors-autentisering om klassningen kräver det.

9.2.3 Hantering av privilegierade åtkomsträttigheter (”Admin”)

Åtkomst med utvidgade rättigheter, så kallade administratörsrättigheter, ska begränsas till så få personer som möjligt. Inloggning med administratörsrättigheter ska alltid ske med ett personligt inloggningskonto.

Behörigheter ska vara begränsade till vad som krävs för att utföra de arbetsuppgifter användaren har. Samma identitet ska inte användas för t ex drift, systemadministration och vanlig användning.

9.2.4 Hantering av användares inloggningsuppgifter

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 och spärras.

9.2.5 Granskning av användares behörigheter och åtkomsträttigheter

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

9.2.6 Borttagning eller justering av behörigheter och 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 anmäla denna typ av förändring.

9.3 Användaransvar

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

9.3.1 Användning av inloggningsuppgifter

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 och spärras.

9.4 Styrning av åtkomst till information, informationssystem och tjänster

Syfte: Att förhindra obehörig åtkomst till information, informationssystem och tjänster.

Den som är inloggad i ett informationssystem ansvarar för vem som tar del av informationen som aktuell inloggning ger åtkomst till.

9.4.1 Begränsning av åtkomst till information

Tillgång till information och informationssystem ska vara begränsad till aktuell roll och det arbete man utför.

9.4.2 Säkra in- och utloggningsrutiner

Regler för att logga in och ut ska finnas för att minimera risken för obehörig åtkomst. Information med hög konfidentialitet som t.ex. känsliga personuppgifter skall skyddas med stark autentisering eller så kallad tvåfaktorsinloggning. Om åtkomst till känsliga personuppgifter sker över öppet nät ska stark autentisering användas.

9.4.3 Lösenordshantering

En robust och genomtänkt hantering av användares lösenord är en förutsättning för att säkra informationen i kommunens processer och system.

Använd unika lösenord för alla företagstillgångar. Implementera bästa praxis både för konton som använder flerfaktorsautentisering och för konton som inte använder det.

Användaren ansvarar för att

- välja ett bra lösenord utifrån givna anvisningar
- hålla lösenordet för sig själv
- inte återanvända lösenordet utanför tjänsten
- vara uppmärksam på missbruk av eget konto, t.ex. senaste inloggning
- uppdatera sin kontaktinformation för återställande av lösenord

Informationsägaren ansvarar för att

- systemet är konfigurerat så att rätt beteende kring lösenord understöds
- förebygga och övervaka dålig efterlevnad, såsom delad användning av konto

IT ansvarar för att

- förebygga val av särskilt olämpliga lösenord, t.ex. namn eller ord
- bevaka intrångsförsök
- dokumentera incidenter

Chefer ansvarar för att medarbetare blir uppmärksammade på och motiverade att ta sitt ansvar. Där så är möjligt bör användaren legitimeras med fler faktorer än bara ett lösenord. Det är användarens ansvar att utnyttja sådana lösningar där de är tillgängliga och det är kommunens ansvar att, i synnerhet vid nyanskaffning av system, minska beroendet av statiska lösenord.

9.4.4 Systemsäkerhet

Informationssystemen skall så långt som möjligt vara konfigurerade och härdade så att det inte går att kringgå säkerhetsfunktionerna. Eventuella undantag från detta kan beslutas av systemägare och då först efter dokumenterad riskanalys.

Oskarshamns kommun

10 KRYPTERING

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

10.1 Kryptografiska säkerhetsåtgärder

10.1.1 Regler för användning av kryptering

Beslut om krypteringslösning ska tas om det bedöms som en lämplig säkerhetsåtgärd baserad på informationsklassning och riskbedömning.

10.1.2 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.

11 FYSISK OCH MILJÖRELATERAD SÄKERHET

Detta kapitel beskriver vad som ska omfattas och beaktas angående fysisk och miljörelaterad säkerhet för informationssystem, informationstillgångar och tjänster i egna lokaler såväl som extern drift.

11.1 Säkra områden

Syfte: Att förhindra otillåten fysisk åtkomst till, skador på och störningar i tillgången till kommunens information, informationssystem och tjänster.

11.1.1 Fysiska säkerhetsavgränsningar

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

11.1.2 Fysiska tillträdesbegränsningar

Säkra områden ska skyddas genom lämpliga säkerhetsåtgärder för att säkerställa att endast behörig personal får tillträde. Loggningsfunktion för tillträde till prioriterade utrymmen som till exempel serverrum ska finnas och vara möjlig att följa upp.

11.1.3 Säkerställande av kontor, rum och anläggningar

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

11.1.4 Skydd mot yttre och miljörelaterade hot

Fysiskt skydd ska utformas och införas för att motverka effekterna av naturkatastrofer, illvilliga angrepp eller olyckor.

11.1.5 Arbeta i säkra utrymmen

Rutiner för arbete i säkra utrymmen ska finnas.

Oskarshamns kommun

11.2 Utrustning

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

11.2.1 Placering och skydd av utrustning

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

11.2.2 Tekniska försörjningssystem

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

11.2.3 Kablagesäkerhet

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

11.2.4 Underhåll av utrustning

Utrustning ska underhållas korrekt för att säkerställa fortsatt tillgänglighet och riktighet. Utrustning i detta avseende är primärt tekniska försörjningssystem men kan även bestå av andra delar.

11.2.5 Utförsel av tillgångar

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

11.2.6 Säkerhet för utrustning och tillgångar utanför organisationen

Säkerhet ska tillämpas på tillgångar utanför organisationens lokaler med hänsyn tagen till de särskilda risker som är förknippade med att arbeta utanför organisationens lokaler.

11.2.7 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.

11.2.8 Obevakad utrustning som hanteras av användare

Användare ska säkerställa att obevakad utrustning har lämpligt skydd.

12 DRIFTSÄKERHET

Detta kapitel beskriver drift och underhåll av informationssystem.

12.1 Driftrutiner och ansvar

Syfte: 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, enligt processer och anvisningar baserade på tillämpliga delar av ITIL.

12.1.1 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.

12.1.2 Ändringshantering

Förändringar i informationssystem och tjänster som påverkar informationssäkerheten ska styras. Processen för ändringshantering bör baseras på ITIL.

12.1.3 Kapacitetshantering

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

12.1.4 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. Säkerhetsreglerna för produktionsmiljöerna ska i relevanta delar även gälla för övriga miljöer.

Oskarshamns kommun

12.2 Skydd mot skadlig kod

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

12.2.1 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.

Installera programvara för antivirus på alla hårdvarutillgångar där det är möjligt, med automatiska uppdateringar mot skadlig programvara.

12.3 Säkerhetskopiering

Syfte: Att skydda mot förlust av data.

12.3.1 Säkerhetskopiering av information

Säkerhetskopiering av information och informationssystem ska utföras regelbundet.

Kopiorna ska förvaras i olika brandceller och med implementerade skyddsåtgärder i enlighet med informationens klassificering. Tester för att återskapa information från säkerhetskopior ska genomföras regelbundet och resultatet ska dokumenteras.

Upprätta och underhåll en process för dataåterställning.

12.4 Loggning och övervakning

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

12.4.1 Loggning av händelser

Det är informationsägarens ansvar att loggning sker så att det i efterhand går att följa enskilda användaraktiviteter, avvikelser, fel och informationssäkerhetshändelser.

Systematiska och regelbundna stickprovskontroller ska göras av loggarna.

Vid hantering av information, klassificerad enligt klassificeringsmodellen, ska loggarna sparas i enlighet med kraven på spårbarhet för det aktuella informationssystemet.

12.4.2 Skydd av logginformation

Loggarna ska vara skyddade mot obehörig åtkomst och manipulation samt finnas tillgängliga utifrån verksamhetens behov.

12.4.3 Administratörs- och operatörsloggar

Systemadministratörers och systemoperatörers aktiviteter ska loggas och loggarna ska skyddas och granskas regelbundet.

12.4.4 Synkronisering av tid

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

12.5 Styrning av informationssystem

Syfte: Att säkerställa riktigheten hos informationssystem.

12.5.1 Installation av program

Rutiner ska finnas för att styra installation av programvara på informationssystem.

12.6 Hantering av tekniska sårbarheter

Syfte: Att förhindra utnyttjande av tekniska sårbarheter.

12.6.1 Hantering av tekniska sårbarheter

Information om tekniska sårbarheter i de informationssystem som används ska löpande bevakas. Exponering för sådana sårbarheter analyseras och lämpliga åtgärder vidtas för att behandla den tillhörande risken.

Det ska finnas en dokumenterad process för sårbarhetshantering.

12.6.2 Användares restriktioner för installation av program

Okontrollerad installation av program kan leda till införande av sårbarheter och leda till obehörig åtkomst till information, förlust av riktighet, andra säkerhetsincidenter eller överträdelse av immateriella rättigheter. Regler för programinstallationer som utförs av användare ska upprättas och införas.

12.7 Överväganden gällande revision av informationssystem

Syfte: Att minimera revisionsverksamhetens påverkan på informationssystem.

12.7.1 Tekniska revisionskontroller för informationssystem

Revision av informationssystem (t.ex. penetrationstester) ska planeras noga och godkännas för att minimera störningar i verksamhetsprocesser. Behov av åtkomst till data i samband med revision ska analyseras och regler för åtkomst ska tillämpas.

För de mest verksamhetskritiska systemen ska revision genomföras regelbundet enligt systemförvaltningsplan. Som verksamhetskritiskt räknas system som klassats med konsekvensnivån ”Allvarlig skada” i minst en av kategorierna Konfidentialitet, Riktighet eller Tillgänglighet.

Oskarshamns kommun

13 KOMMUNIKATIONSSÄKERHET

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

13.1 Hantering av nätverkssäkerhet

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

13.1.1 Säkerhetsåtgärder för nätverk

Nätverk ska hanteras och styras på ett sådant sätt att information i informationssystem och tjänster skyddas.

13.1.2 Säkerhet hos nätverkstjänster

Nätverkstjänster omfattar anslutningar och nät med värdeskapande tjänster samt nätverkssäkerhetslösningar som t.ex. brandväggar och intrångsdetekteringssystem. 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.

13.1.3 Separation av nätverk

Grupper av informationstjänster, användare och informationssystem ska separeras i nätverk. Separation av nätverk kan vara så väl logisk som fysisk.

13.2 INFORMATIONSÖVERFÖRING

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

13.2.1 Regler och rutiner för informationsöverföring

Det ska finnas regler, rutiner och skyddsåtgärder för att skydda information vid överföring, så väl inom kommunen som till en extern enhet.

13.2.2 Överenskommelser om informationsöverföring

Överföring av information mellan kommunen och externa parter ska vara reglerad i överenskommelser som återspeglar informationens klassning.

13.2.3 Elektronisk meddelandehantering

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

Använd endast godkända webbläsare och e-postklienter. Blockera onödiga filtyper för inkommande epost.

14 DATASKYDD

Detta kapitel beskriver specifikt hanteringen av personuppgifter.

14.1 Hantering av personuppgifter

Syfte: Detta kapitel beskriver hur personuppgifter ska hanteras och förtydligar ansvarsförhållandet angående personuppgiftshantering.

14.1.1 Personuppgiftansvar

Oskarshamns kommuns samtliga nämnder samt styrelser i sådana organisationer där Oskarshamns kommun har det rättsligt bestämmande inflytandet, är personuppgiftsansvariga för sina respektive verksamhetsområden.

Ansvaret innebär en yttersta skyldighet att tillse att gällande lagstiftning efterlevs genom att

- Fastställa ändamål och syfte med behandling av personuppgifter, innan behandling påbörjas
- Utse Dataskyddsombud och svara för att denne har förutsättningar och besitter erforderlig kunskap och för att fullgöra sitt uppdrag
- Säkerställa att det finns tekniska och organisatoriska förutsättningar att behandla personuppgifter med erforderlig säkerhet
- Kunna visa att kraven i lagstiftningen är uppfyllda genom noggrann dokumentation samt verifierande tester
- Föra register över behandlingar av personuppgifter

14.1.2 Behandling av personuppgifter

Personuppgifter får endast behandlas om det finns laglig grund för behandlingen. Den lagliga grunden ska fastställas innan behandling påbörjas enligt någon av nedan punkter:

- Behandlingen är nödvändig för att fullgöra ett avtal
- Behandlingen är nödvändig för att fullgöra en rättslig förpliktelse som den personuppgiftsansvarige har
- Behandlingen är nödvändig för att skydda ett grundläggande intresse för den registrerade eller annan fysisk person
- Behandlingen är nödvändig för att utföra en uppgift av allmänt intresse eller som ett led i den personuppgiftsansvariges myndighetsutövning
- Samtycke – ska vara informerat, frivilligt och specifikt samt kunna visas.

14.1.3 Säkerhet inom dataskydd

Behandling av personuppgifter får ske om lämplig teknisk och organisatorisk säkerhet vidtagits för behandlingen. Säkerheten ska baseras på genomförda informationssäkerhetsklassningar och riskanalyser.

Säkerhet utifrån personuppgiftshantering utgörs av:

- Inbyggt dataskydd och dataskydd som standard
- Införande och tillämpning av rutiner

Inbyggt dataskydd och dataskydd som standar innebär:

- att säkerställandet av personuppgiftshanteringen ska finnas med redan från den initiala planeringen och täcka såväl tekniska som organisatoriska åtgärder
- säkerställa att kommunens grundsäkerhetsnivå för informationssäkerhet (nivå 1) föreligger samt om möjligt nyttja åtgärder som pseudonymisering, anonymisering eller kryptering
- säkerställa att kommunens förhöjda säkerhetsnivå för informationssäkerhet föreligger avseende särskilda personuppgifters konfidentialitet och riktighet vilket för elektronisk hantering bl.a. innebär nyttjande av kryptering samt stark autentisering för e-legitimation
- nyttja åtgärder som uppgiftsminimering, lagringsminimering, fritextfältsminimering och åtkomstbegränsning

Införande och tillämpning av rutiner innebär:

- Kontinuerligt testa, undersöka och visa på effektiviteten av införda säkerhetsåtgärder
- Anmäla personuppgiftsincident till tillsynsmyndighet
- Vid behov kunna ge incidentinformation till berörda registrerade
- Vid behov kunna involvera och rådgöra med dataskyddsombudet

14.1.4 Vid användande av personuppgiftsbiträde

Den som behandlar personuppgifter på uppdrag av annan personuppgiftsansvarig blir personuppgiftsbiträde i förhållande till den personuppgiftsansvarige. Vid anlitandet av ett personuppgiftsbiträde ska det säkerställas att denne kan ge tillräckliga garantier om att upprätthålla lämplig teknisk och organisatorisk säkerhet i enlighet med gällande rätt.

Personuppgiftsbiträdets behandling av personuppgifter ska regleras av personuppgiftsbiträdesavtal mellan biträdet och den personuppgiftsansvarige. Innan inträde av avtal ska personuppgiftsansvarig rådfråga informationssäkerhetssamordnare, Dataskyddsombud eller annan roll med kunskap i dataskydd och avtalsskrivande.

14.1.5 Särskilt skydd av personer med skyddade personuppgifter

Varje personuppgiftsansvarig måste vidta lämpliga tekniska och organisatoriska åtgärder för att hantera alla personuppgifter som behandlas i organisationen. En säker hantering av skyddade personuppgifter bygger på säkra IT-system och begränsad tillgång till skyddade personuppgifter. Det ska också finnas tydliga rutiner för hur personalen ska hantera skyddade personuppgifter.

Oskarshamns kommun

15 SÄKER LIVSCYKEL HOS INFORMATIONSSYSTEM

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

15.1 Säkerhetskrav på informationssystem

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

15.1.1 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.

15.1.2 Säkerhetskrav på publika tjänster

Informationssystem på publika nätverk kräver specifika säkerhetsöverväganden mot typiska nätverksrelaterade hot som röjande av information för obehöriga, bedrägliga transaktioner och belastningsattacker. Det ska ske genom detaljerade riskbedömningar och val av motiverade säkerhetsåtgärder.

Transaktioner ska skyddas för att förhindra ofullständig överföring, felaktig styrning av nätverkstrafik, obehörig ändring av meddelanden eller obehörigt röjande.

15.2 Säkerhet i utvecklings- och supportprocesser

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

15.2.1 Regler för säker utveckling

Regler för utveckling av informationssystem och tjänster ska upprättas och tillämpas. Processen ska även omfatta säkerhet i egenutvecklade applikationer.

15.2.2 Rutiner för hantering av ändringar i informationssystem och tjänster

Vid införande eller vid större ändringar av informationssystem och tjänster ska en formell process för ändringshantering följas. Processen ska omfatta test och verifiering samt riskanalys och specificering av nödvändiga säkerhetsåtgärder.

15.2.3 Rutiner för hantering av ändringar i driftsmiljö

Vid större ändringar i driftmiljön ska en formell process för ändringshantering följas.

Processen ska omfatta test och verifiering samt riskanalys och specificering av nödvändiga säkerhetsåtgärder, för att säkerställa att det inte innebär negativ påverkan på verksamheten eller säkerheten.

15.2.4 Restriktioner för ändringar av programpaket

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

15.2.5 Principer för utveckling av säkra informationssystem

Informationssäkerhet ska beaktas vid utveckling av informationssystem. Styrdokument för utveckling av säkra system bör upprättas, dokumenteras, underhållas och tillämpas vid utveckling av säkra informationssystem.

15.2.6 Säker utvecklingsmiljö

Kommunen ska bedöma riskerna med utvecklingsarbete för enskilda system och upprätta säkra utvecklingsmiljöer för specifika system. I utvecklingsprocesser ska informationssystem skyddas på motsvarande sätt som produktionsmiljön.

15.2.7 Outsourcad utveckling

Kommunen ska övervaka och styra outsourcad systemutveckling.

15.2.8 Systemtest med inriktning säkerhet

Vid systemtest ska tester genomföras för att verifiera att ställda krav på informationssäkerhet är uppfyllda.

15.2.9 Acceptanstestning av informationssystem och tjänster

Process för acceptanstest, driftgodkännande och produktionssättning ska finnas och användas. Informationssystem och tjänster ska genomgå acceptanstest före driftgodkännande av beställare. I driftgodkännandet ska det ingå en uppföljning av säkerhetskraven.

15.3 Testdata

Syfte: Att säkerställa skyddet av data som används för tester.

15.3.1 Skydd av testdata

Verksamhetsinformation som innehåller personinformation eller annan konfidentiell information bör inte användas för teständamål. Om personinformation eller annars konfidentiell information används för testning bör alla känsliga detaljer och innehåll tas bort eller ändras.

Oskarshamns kommun

16 LEVERANTÖRSRELATIONER

Syfte: Detta kapitel beskriver vad som ska omfattas och beaktas i leverantörs-relationer för att säkerställa skydd av kommunens informationstillgångar.

16.1 Informationssäkerhet i leverantörsrelationer

16.1.1 Informationssäkerhetsregler för leverantörsrelationer

När kommunen köper IT-tjänster av extern part eller förlägger drift av informationssystem och tjänster hos en sådan, ska minst samma regler för informationssäkerhet gälla och avtalas som när driften hanteras i egen regi.

16.1.2 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.

16.1.3 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.

16.2 Hantering av leverantörers tjänsteleverans

Inventera samtliga tjänsteleveranser. Avtal med tjänsteleverantörer ska innehålla säkerhetskrav.

16.2.1 Övervakning och granskning av leverantörstjänster

För de tjänsteleveranser som klassificeras som verksamhetskritiska ska kommunen regelbundet övervaka, granska och genomföra revision.

16.2.2 Ändringshantering av leverantörers tjänster

Vid ändring av leverantörers tjänster eller avtal ska en förnyad riskbedömning genomföras. Avveckla tjänsteleverantörer på ett säkert sätt. Säkerställ att information gallras eller överförs på ett kontrollerat sätt till kommunen.

Oskarshamns kommun

17 HANTERING AV INFORMATIONSSÄKERHETSINCIDENTER

17.1 Hantering av incidenter och förbättringar

17.1.1 Ansvar och rutiner

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

17.1.2 Rapportering av informationssäkerhetsincident

Alla användare, anställda och leverantörer ska göras medvetna till sin skyldighet till, och även uppmuntras att rapportera informationssäkerhetsincidenter så snabbt som möjligt.

17.1.3 Rapportering av svagheter gällande informationssäkerhet

Anställda och leverantörer som använder kommunens informationssystem och tjänster ska rapportera alla observerade eller misstänkta svagheter gällande informationssäkerheten.

17.1.4 Bedömning av och beslut om informationssäkerhetsincidenter

Informationssäkerhetshändelser ska bedömas och beslut ska fattas om de ska klassificeras som informationssäkerhetsincidenter. Resultaten av bedömningar och beslut ska dokumenteras detaljerat för framtida referens och verifiering.

17.1.5 Hantering av informationssäkerhetsincidenter

Informationssäkerhetsincidenter ska hanteras enligt beslutade processer, se ”Rutin för incidenthantering”.

17.1.6 Att lära av informationssäkerhetsincidenter

Informationsägaren ansvarar för att hanterade informationssäkerhetincidenter analyseras och att kunskapen om dessa används för att minska sannolikhet för framtida skador.

17.1.7 Insamling av bevis

Kommunen ska fastställa och tillämpa rutiner för identifiering, insamling, kopiering och bevarande av information som kan tjäna som bevis. Informationen ska sparas minst till dess att allvarlighetsgraden i händelsen är helt klarlagd.

18 VERKSAMHETENS KONTINUITET

18.1 Kontinuitet för informationssäkerhet

Syfte: Kontinuiteten för informationssäkerhet är integrerad i kommunens verksamhetsprocesser.

18.1.1 Planering av kontinuitet för informationssäkerhet

Med kontinuitetsplanering avses den planeringsprocess som syftar till att säkerställa fortsatt verksamhet vid störningar och avbrott i informationssystem och tjänster, som beskrivs i en avbrottsplan.

18.1.2 Införa kontinuitet för informationssäkerhet

Kommunens processer, rutiner och säkerhetsåtgärder ska säkerställa den nivå av kontinuitet för informationssäkerhet som anges i avbrottsplanen.

18.1.3 Styra, granska och utvärdera kontinuitet för informationssäkerhet

Kommunen ska verifiera de fastställda och införda åtgärderna för kontinuitet av informationssäkerhet med jämna mellanrum för att säkerställa att de är giltiga och verkningsfulla under störningar.

18.2 Redundans

Syfte: Att säkerställa tillgänglighet till information, informationssystem och tjänster.

18.2.1 Tillgänglighet för informationssystem

För informationssystem med hög säkerhetsnivå på tillgänglighet bör den befintliga systemarkitekturen kompletteras med redundanta enheter eller redundant arkitektur.

19 EFTERLEVNAD

19.1 Efterlevnad av juridiska och avtalsmässiga krav

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

19.1.1 Identifiering av gällande lagstiftning och avtalsmässiga krav

Alla krav som återfinns i lagar, förordningar och/eller avtal som berör kommunen ska identifieras och dokumenteras i syfte att uppfylla kraven.

19.1.2 Immateriella rättigheter

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

19.1.3 Skydd av dokumenterad information

Dokumenterad (lagrad) information ska skyddas från förlust, förstörelse, förfalskning, obehörig åtkomst och otillåten utgivning enligt informationens säkerhetsklassning, oavsett media.

19.1.4 Reglering av kryptografiska säkerhetsåtgärder

Kryptografiska säkerhetsåtgärder ska användas i enlighet med gällande avtal och författningar. Se kapitel 10 Kryptering.

19.2 Mätning och granskning av informationssäkerhet

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

19.2.1 Löpande mätning av säkerhet och säkerhetsincidenter

Kommunens processer och system, liksom yttre krav och förväntningar, utvecklas ständigt. Att upprätthålla rätt säkerhet förutsätter mätning, dels av den uppnådda säkerhetsnivån

(åtminstone upptäckta incidenter) och dels av det säkerhetsrelaterade arbete som utförts (åtminstone dokumenterade riskanalyser) respektive inte utförts.

19.2.2 Extern granskning

Kommunens tillvägagångssätt för att hantera informationssäkerhet och dess införande ska med jämna mellanrum eller när betydande förändringar sker genomgå oberoende granskning.

Extern granskning ska avse olika typer av säkerhetstester, som penetrationstester.

19.2.3 Intern granskning

Informationssäkerhetsansvarig ska regelbundet granska efterlevnaden av informations-säkerhetspolicyn, gällande regler och riktlinjer, standarder och eventuella andra säkerhetskrav. En utgångspunkt är de mätetal som definierats.

19.2.4 Granskning av teknisk efterlevnad

Informationssystem och tjänster ska granskas regelbundet avseende teknisk efterlevnad. Detta görs normalt med hjälp av automatiserade verktyg som genererar tekniska rapporter som tolkas av en teknisk specialist.