Informationssäkerhet

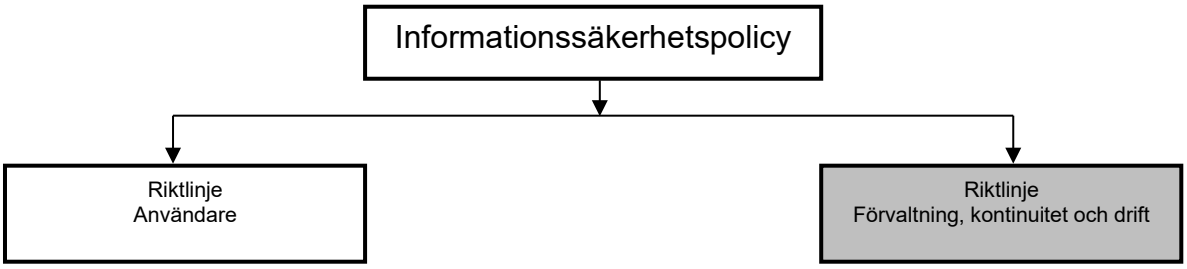
Riktlinje – Förvaltning, kontinuitet och drift

Fastställda av kommunchefen 2018-01-22, då tidigare riktlinjer antagna 2011-06-20 upphör att gälla

Innehåll

1 Informationssäkerhet

Styrande dokument för informationssäkerhetsarbetet är Ale kommuns informationssäkerhetspolicy och riktlinjerna Användare och Förvaltning, kontinuitet och drift.



Informationssäkerhetspolicyn redovisar ledningens viljeinriktning och mål för informationssäkerhetsarbetet. Riktlinjen Förvaltning, kontinuitet och drift utgår från policyn och syftar till att redovisa:

- den interna organisationen för informationssäkerhetsarbetet enligt Förvaltningsmodell IT
- omfattningen av det ansvar som vilar på driftorganisationen för informationssäkerhetsarbetet
- hur informationssäkerhetsarbetet ska bedrivas
- de generella krav som är aktuella

2 Organisation och ansvar för säkerhetsarbetet

2.1 Säkerhetschef

Finns en rollbeskrivning i informationssäkerhetsarbetet.

Har huvudansvaret för samordning av informationssäkerhetsarbetet och är utsedd av kommunchefen.

- Ansvara för att policy och riktlinjer för informationssäkerhetsarbetet utarbetas och beslutas.
- Övervaka att policy och riktlinjer för informationssäkerhetsarbetet följs och vid behov föreslå förbättringar.
- Ta initiativ till och medverka i informations- och utbildningsaktiviteter gällande informationssäkerhet.
- Kontrollera att befintliga säkerhetsregler följs och vid behov föreslå förbättringar
- Initiera informationssäkerhetsrevisioner.
- Kontinuerligt rapportera till förvaltningsledningen om status för informationssäkerhetsarbetet.

2.1.1 Arbetsgrupp för informationssäkerhetsarbetet

Säkerhetschefen (administrativ chef vid sektor kommunstyrelsen) ansvarar för informationssäkerhetsarbetet i samråd med IT-chefen.

Det finns en referensgrupp bestående av

- Representant utsedd av IT-chef
- Handläggare utsedd av administrativ chef
- Arkivarie
- Säkerhetssamordnare
- Representant utsedd av kommunikationschef
- Dataskyddsombud

Gruppen sammankallas av säkerhetschefen och träffas normalt fyra gånger om året.

Säkerhetschefen svarar för

att ta fram förslag till regler, riktlinjer och policies inom området och att nödvändig information kring verksamheten finns på kommunens webbplats och intranät.

att en gång varje år rapportera det gångna årets arbete kring informationssäkerheten och notera eventuella incidenter och avvikelser till kommunchefen.

att rapportera vid behov eventuella incidenter och avvikelser till förvaltningsledningen och föreslår också de åtgärder som behövs och genomför dessa efter beslut.

2.2 IT-chef

IT-chefen är ägare av Förvaltningsmodell IT och objektsägare för Teknisk plattform och IT-arbetsplats. Därutöver ansvarar IT-chefen för att

- sammankalla alla objektsägare till objektsägarmöte
- den tekniska plattformen fungerar
- identifiera de delar som ingår samt att en säkerhetsanalys genomförs
- en kontinuitetsplan för driften av IT-verksamheten upprättas samt att den senare integreras med Ale kommuns övriga kontinuitetsplaner
- endast behöriga får tillträde till IT-verksamhetens fysiska utrymmen

2.3 Sektorschef

Sektorschef ansvarar för att personalen har tillräckliga kunskaper för att hantera information på ett säkert sätt.

2.4 Närmaste chef

Användarens närmsta chef ansvarar för att

- beställning och avbeställning av behörigheter för sin personal.
- nödvändig utbildning genomförs.
- i samband med nyanställning, omplacering och om speciella behov föreligger genomföra utbildningar inom informationssäkerhetsområdet

2.5 Förvaltningsmodell-IT

En beskrivning av rollerna finns i Riktlinjer för förvaltningsmodell IT på intranätet.

2.6 Användare

Användare är varje person som har behörighet till informationstillgångarna.

- ansvarar för att följa kommunens gällande policy och riktlinjer för informationssäkerhet och för respektive informationstillgång.

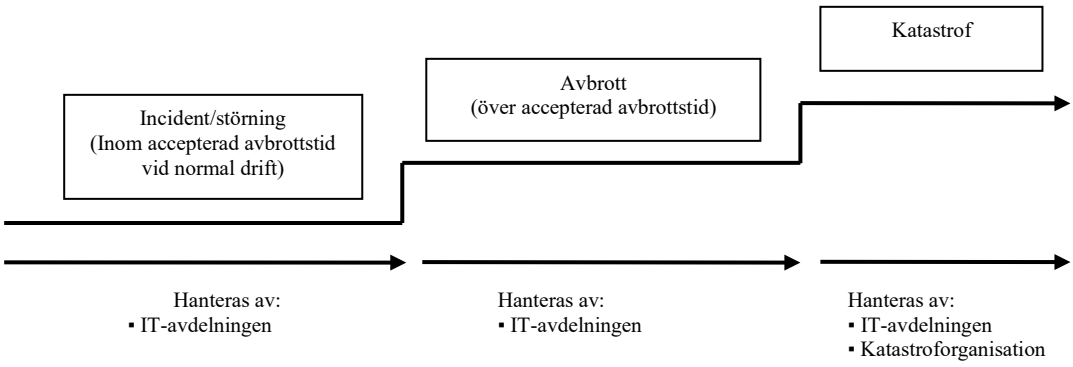
3 Hantering av informationstillgångar

3.1 Vad är en informationstillgång

Enligt SIS Handbok 550 är informationstillgångar en organisations information och de resurser som används för att hantera informationen, t ex programvaror, tjänster och fysiska tillgångar.

3.2 Hantering av incident/störning

Nedanstående modell beskriver hur avbrott hanteras under olika faser av störningar/avbrott.



Incident/Störning
En oönskad händelse som kan hanteras inom accepterad avbrottstid med interna eller externa resurser

Avbrott
En oönskad händelse som inte kan hanteras inom accepterad avbrottstid med interna eller externa resurser

Katastrof
En mycket allvarlig händelse bortom all kontroll och som kraftigt påverkar verksamheten

3.2.1 IT-Support

- IT-support är bemannad dagtid och utgör grunden i IT-funktionen och ska
- Ta emot anmälan om alla typer av händelser.
- Upprätta dagbok med utrymme för tidpunkt för anmälan, vem anmälde, och om möjligt hur händelsen uppstod eller upptäcktes.
- Klassificera incidenter.
- Hantera incidenter och störningar.

Hos IT-support ska minst finnas:

- Förteckning över resurspersoner
- Förteckning över aktuella kontaktpersoner inom förvaltningsorganisationen.

3.2.2 IT-tekniker i beredskap

Utanför kontorstid tillhandahålls beredskap för att kunna vidta åtgärder vid incidenter av mer allvarlig händelse. Med allvarlig händelse avses fel som berör stor del av kommunens verksamhet eller som är av stor ekonomisk eller imagemässig betydelse för kommunen; eller att system/tjänster helt eller delvis inte kan användas. (Avbrottet ska avse system som har klassats som

verksamhetskritiska, exempelvis att Ales webbplats ej går att nå eller att verksamhetssystem inom vårdsektorn är nere.).

Fel som berör enskilda användare eller tjänst/funktioner och inte påverkar verksamheten i någon större grad ska inte åtgärdas utanför kontorstid.

3.3 Ansvar för tillgångar

Det ska finnas en tydlig ansvarsfördelning för samtliga informationstillgångar och dessa dokumenteras i förvaltningsplanen.

Kommunens IT-utrustning ska innan leverans märkas och dokumenteras av IT-avdelningen.

För nybeställning och avslut av IT-utrustning och informationstillgångar till användare ansvarar berörd chef.

Namnstandarder ska finnas och följas för arbetsstationer, servrar, nätverksutrustning och övrig utrustning.

3.4 Klassificering av informationstillgångar

Informationstillgångar i Ale kommun ska klassas utifrån den information som hanteras i respektive tillgång. Objektsledaren ansvarar för att klassningen genomförs.

Klassningen ska genomföras efter Ale kommuns klassningsmodell. Klassningen genomförs utefter aspekterna konfidentialitet, sekretess, tillgänglighet och riktighet. Vid förändringar i tillgångens innehåll ska en ny klassning med riskanalys genomföras och dokumenteras i system för beslutsstöd.

Med detta menas:

- Konfidentialitet: Om röjd information kan påverka enskilda personer eller andra organisationer.
- Riktighet: Information är skyddad mot oavsiktlig och avsiktlig förvanskning.
- Tillgänglighet: Hur lång tid kan medarbetare och externa intressenter vara utan tillgång till informationen?
- Spårbarhet: Ändringar, justeringar, radering mm i systemet ska vara möjliga att tyda och följa i efterhand.

Tas information ut ur något system och lagras på andra media, eller används i annat sammanhang, måste den klassas där den används och hanteras därefter.

3.4.1 Informationsklassificeringsmodell

Information kring modellen finns i Rutin för informationssäkerhetsarbetet.

3.5 Hantering av skyddad identitet

I våra informationstillgångar kan det förekomma personer med skyddad identitet. Skyddad identitet är en metod för att skydda personer som är utsatta för ett konkret och allvarligt hot. Det är därför av största vikt att Ale kommun hanterar dessa uppgifter på ett korrekt och säkerhetsmedvetet sätt.

HR och Elevadministrativa systemen har ett grundläggande ansvar när det gäller hantering av alla identiteter. IT har en tjänst som skapar upp konton för elever och personal. Personer med skyddad identitet skapas upp på samma sätt som för övriga. Om det finns specifika önskemål tas kontakt med IT-avdelningen som hanterar detta. Varje objektägare ansvarar för hanteringen i sina verksamhetssystem.

4 Fysisk och miljörelaterad säkerhet

4.1 Säkrade utrymmen

Det är viktigt att vi fysiskt skyddar den utrustning som hanterar vår information. Vårt fysiska skydd ska förhindra obehörigt tillträde, skadegörelse och störningar i organisationens lokaler och informationsutrymmen.

4.1.1 Tillträdesskydd

Endast utsedd och behörig personal har tillgång till serverhallar och utrymmen med känslig information. Tillträdet registreras genom loggning i passagesystemet och dessa uppgifter hanteras i enlighet med gällande rutin.

I utrymmen med känslig information ska extern personal som till exempel servicepersonal, städpersonal med flera endast ges tillträde när det är nödvändigt. Besöksmottagaren ansvarar för att extern personal övervakas när behovet föreligger.

Dessa utrymmen ska vid behov även förses med kontroll för in- och utpassering. Tillträdet ska registreras och dessa uppgifter förvaras säkert. Ansvarig chef ansvarar för att utrymmena är säkrade.

4.1.2 Brandskydd

Datorer och annan elektronisk utrustning som lagringsmedia är känsliga för brand, annan temperaturhöjning och rök. Det är viktigt att ett ändamålsenligt skydd finns i de utrymmen där sådan utrustning finns.

4.1.3 Vattenskydd

Rör där vatten står under tryck bör inte finnas i säkra utrymmen. Vätskelarm ska finnas om det i utrymmet finns rördragningar innehållande vatten eller om det av andra orsaker finns risk för vattenskada.

4.1.4 Klimatanläggning

Temperaturen ska kunna mätas och regleras. Leverantörens rekommenderade underhållsplan för utrustningen ska i första hand följas.

4.1.5 Elförsörjning

Utrustning som kan behöva förses med avbrottsfri kraft (UPS) kan vara servrar, som exempelvis nätverksservrar, samt kommunikationsutrustning. Generellt är det tillräckligt om centrala servrar och datakommunikationsutrustningar skyddas mot ett elbortfall på cirka ett par timmar.

IT-avdelningen ska ombesörja att utrustning för avbrottsfri kraft (UPS) är i funktionsdugligt skick. UPS ska testas minst 2 gånger per år och dokumenteras.

Ale elförening ska enligt avtal med Ale kommun svara för att reservkraftsaggregat finns för användande då kommunhuset i Alafors blir utan strömförsörjning med anledning av kortare eller längre avbrott i elleveransen. Denna anläggning ska testas minst 1 gånger per år och dokumenteras. Ansvar för att detta arbete sker från Ale Elförenings sida åvilar Internservice.

5 Styrning av kommunikation och drift

5.1 Driftdokumentation

Driftdokumentation finns upprättad av IT-avdelningen. Den ska i en rimlig omfattning vara fullständig och aktuell samt uppdateras vid förändringar i infrastruktur och verksamhetssystem. Dokumentationen finns i IT-avdelningens säkerhetswebbplats och dokumenteras utifrån respektive verksamhetshetssystem. Driftdokumentationen ska förvaras skyddad och åtskild från driftstället.

Driftdokumentationen bör minst omfatta:

- Installations- och konfigurationsinstruktioner, inställningar av olika parametrar i verksamhetssystemet som till exempel förändringar av default-inställningar i operativsystem
- Återstarts- och återställningsrutiner
- Övervakning, loggning och hantering av revisionsspår (brandvägg, operativsystem med mera)
- Säkerhetskopiering
- Ändringshantering

5.2 Säkerhetskopiering och återläsning av data

5.2.1 Generella regler avseende säkerhetskopiering och återläsning av filer och epost:

- Återställning av borttagna filer sker via papperskorgen
- 30 dagar efter att man avslutat sin anställning tas alla dokument i onedrive och epost bort och kan inte återställas
- Dokument skapade i grupper kan återställas via papperskorgen och påverkas inte om någon avslutar sin anställning

5.2.2 Generella regler avseende säkerhetskopiering och återläsning av system:

- Återställning av data ska kunna ske från valfri dag enligt generell plan eller speciella beställningskrav, efter begäran från chef.
- För de system som har databaser (för mer aktuell återställning till exempel transaktions¬loggning) sparas dessa i fyra veckor (transaktionsloggarna backas upp en gång per timme).
- Säkerhetskopior förvaras säkert och brandskyddat på annan geografisk plats än källdata.
- Tester för att återskapa information från säkerhetskopior ska genomföras enligt upprättad plan och resultatet ska dokumenteras.

5.2.3 Undantag

Om ingen av dessa nivåer är tillräcklig i förhållande till objektsledaren/-specialistens krav ska en skräddarsydd lösning erbjudas enligt tjänstekatalogen.

Objektsägare ska i samråd med objektsägare-IT ta beslut för informationstillgångarna om:

- vilken information som ska omfattas av säkerhetskopiering
- intervallen för kopiering om inte generella regler används
- hur många generationer säkerhetskopior som ska finnas om inte generella regler används

- när återläsningstester ska genomföras

5.3 Ändringshantering enligt gällande förändringsprocess

Förändringar i driftmiljö, informationstillgångar, utrustning och rutiner ska styras genom Förvaltningsmodell IT som innebär att det finns dokumentation som beskriver:

- ansvarig beställare
- godkännande/beslutsform enligt förändringsprocessen
- identifiering och registrering
- konsekvensanalys
- informationskrav till verksamheten
- Rutin för avbrytande av och återställande av misslyckade ändringar.

Ändringar som bedöms kunna påverka informationssäkerheten ska testas i separat testmiljö innan de införs i produktionsmiljön.

5.4 Skydd mot skadlig kod

Leverantörernas säkerhetsuppdateringar ska installeras fortlöpande. För att säkerställa att driften inte påverkas negativt ska säkerhetsuppdateringar analyseras innan de installeras i produktionsmiljön.

Säkerhetspatchar till operativsystem (till exempel MS Windows, Linux med mera) sker automatiskt. Viruskontroll sker automatiskt och virusdefinitionsfiler uppdateras löpande för att garantera aktuellt skydd. Extra verktyg används för att vara ute i god tid för att stoppa risker i miljön.

5.5 Utbyte av information

Allt externt informationsutbyte avseende informationstillgångar inom och utanför organisationen ska regleras mellan kommunen och den externa parten.

Objektsägaren

- ansvarar för regleringen
- beslutar om vilka åtgärder som ska vidtas vid fysisk transport av för verksamheten känsliga informationstillgångar

Objektägare och objektägare-IT reglerar tillsammans

- driftsättning och godkännande av internet- eller molntjänster

Före beställning av internet- eller molntjänster ska IT-avdelningen kontaktas enligt förändringsprocessen, avsnitt 5.3.

5.6 Kapacitetsplanering

Kapacitetsplanering syftar till att förutse kapacitets- eller prestandaproblem. Regelbunden mätning och uppföljning av kapaciteten ska genomföras. Detta är särskilt viktigt för de system som bedöms som verksamhetskritiska.

Objektledaren/objektspecialisten ska meddela förändringar som planeras till IT-avdelningen

5.7 Loggning, spårbarhet

Loggning av aktivitet i verksamhetsverksamhetssystem ska göras för att kunna spåra vem som har gjort vad. I händelse av att en incident inträffar ska man med hjälpa av loggarna kunna avgöra vem/vilka som antingen har gjort något otillåtet eller begått ett misstag.

Objektsledaren ansvarar för att det finns beslutade regler gällande logghantering för sin informationstillgång och att den finns en förteckning över dessa.

Beslut om logghantering i samband med systemsäkerhetsanalysen ska dokumenteras i förvaltningsplanen.

5.7.1 Regler för loggning

Regler för loggning ska omfatta:

- Syfte med loggarna
- Hur ofta loggar ska analyseras. Analysen sker regelbundet samt med avseende på tecken på onormala förhållanden och säkerhetsincidenter
- Vem som ansvarar för analysen
- Vem som har tillgång till loggarna, då de ska skyddas mot obehörig åtkomst och manipulering
- Hur länge loggarna ska sparas i enlighet med gallringsbeslut, t ex loggar som kan vara integritetskänsliga (t ex övervakningsbilder och – filmer) får endast sparas enligt fattade beslut för respektive område.
- Med hänsyn till gällande lagstiftning avseende hantering av personuppgifter och dataskydd ska loggning begränsas i tid.
- Hur ska loggarna förvaras

5.7.2 Revisionsloggar

Objektsledare ansvarar för att

- verksamhetssystemet är konfigurerat så att revisionsloggar finns för säkerhetsrelevanta händelser.
- tillsammans med objektspecialisten, i de fall det inte är möjligt att logga automatiskt, ska möjlighet till manuell logg finnas, till exempel vid systemfel eller tekniska begränsningar.

Revisionsloggarna ska minst registrera:

- Användaridentitet.
- Datum och tidpunkt för in- och utloggning.
- Lyckade och misslyckade försök till åtkomst.

Revisionsloggar för verksamhetskritiska system ska även registrera:

- Driftoperatörers och systemadministratörers identitet vid inloggning.

- Datum och tidpunkt för driftoperatörers och systemadministratörers inloggning och för sekretesskänsliga system även registrering vid utloggning.
- Driftoperatörers och systemadministratörers lyckade och misslyckade försök till åtkomst.

5.8 Övervakning

Övervakningssystem för övervakning av nätverksenheter såsom servrar, routrar och skrivare ska finnas för att åtgärda driftstörningar innan det blir ett problem för användarna.

En lista på samtliga verksamhetssystem/nätverksutrustning som övervakas och på vad som övervakas med avseende på prestanda ska finnas.

Rutin för gällande övervakningssystem ska finnas dokumenterad som innehåller processen för hantering av larm från övervakningssystemen.

5.8.1 Kameraövervakning

Ska efter godkännande hanteras enligt beslut av objektägaren. Endast behöriga ska ha tillgång till systemet. Loggning dokumenteras enligt 5.9.

5.9 Hantering av säkerhet i nätverk

Kommunens olika nätverk ska vara logiskt separerade. Varje nätverk ska utformas så att det finns definierade gränssnitt, såväl fysiskt som logiskt, mot andra nätverk.

Respektive nätverk bör dessutom vara logisk separerade i så kallade nätverkssegment. Denna separering minskar risken för obehörig åtkomst samt möjliggör uppdelning i åtskilda produktions- och testmiljöer, vilket minskar risken för att testarbete stör produktionen.

Sammankoppling av nätverk får endast ske efter att säkerhetsaspekterna analyserats och nödvändiga skyddsåtgärder vidtagits av respektive nätverks tekniska specialist.

I samband med att information överförs genom data- och telekommunikation, uppkommer risker för avlyssning och förändring av den överförda informationen.

Respektive objektsägare ansvarar för att analysera behov av nödvändiga skyddsåtgärder för att hantera dessa risker och dokumentera dem.

Kablage, aktiva nätverkskomponenter och kommunikationsprotokoll ska väljas med utgångspunkt från verksamhetens krav på informationssäkerhet. Datakommunikationen ska begränsas till vad som krävs för informationsutbytet.

5.10 Hantering av trådlösa nätverk

Trådlösa nätverk inom Ale kommun ska ha en säkerhetslösning som omfattar autentisering och kryptering som integritetskontroll. Som minimum bör WPA2 (Wi-Fi Protected Access) och protokollet 802.1x användas.

6 Styrning av åtkomst

6.1 Styrning av användares åtkomst

Objektledare/objektspecialist ska säkerställa att verksamhetssystemet är konstruerat så att alla rekommendationer avseende behörighetskontroll kan tillgodoses.

Objektledare/objektspecialist ansvarar för behörighetshantering i sitt eget system. Behörigheter för användare som börjar, slutar eller byter arbetsuppgifter ska hanteras när det gäller tilldelning, uppföljning och uppdatering av behörigheter.

Närmaste chef ansvarar för att användare före tilldelning av behörigheter ges tillräckliga kunskaper om gällande säkerhetsinstruktioner och instruktioner som speciellt ansluter till den egna arbetsuppgiften.

6.1.1 Manuell behörighetshantering

Behörighet i verksamhetssystem som inte är kopplade till tjänstekatalog (AD) ska spärras inom en vecka. Minst en gång per år ska det kontrolleras att endast behöriga användare är registrerade i behörighetssystemet för verksamhetssystemet.

6.1.2 Automatisk behörighetshantering via AD

Anställda och inhyrd personal kommer att spärras i AD dagen efter anställningen/uppdraget avslutats. Verksamhetssystem som är kopplade till AD spärras automatiskt i verksamhetssystemet.

Konsulter inaktiveras när de inte är aktiva. Den som aktiverat kontot ansvarar för att inaktivering sker.

6.2 Styrning av IT-personalens åtkomst

IT-chefen ansvarar för behörighetshantering för personal inom IT-avdelningen. Behörigheter för personal inom IT-avdelningen och konsulter som börjar, slutar eller byter arbetsuppgifter ska hanteras. Detta omfattar godkännande, uppföljning och uppdatering av behörigheter.

Åtkomst med utvidgade rättigheter, så kallade administratörsrättigheter, som möjliggör för användaren att till exempel ändra rättigheter eller konfigurationer i applikationer, databaser, operativsystem eller nätverk ska begränsas till så få personer som möjligt.

Systemadministrativa arbetsuppgifter ska alltid vara kopplade till personliga användaridentiteter för att säkerställa spårbarhet avseende genomförda aktiviteter. För administratörer med omfattande behörigheter, där ovanstående inte kan tillämpas, ska särskilda skyddsåtgärder vidtas, till exempel upprättande av manuell åtkomstlogg.

6.3 Styrning av åtkomst till nätverk

IT-avdelningen ansvarar för och administrerar brandväggarna enligt krav från objektsägaren-IT. Förändringar i brandväggen ska ske i enlighet med förändringshanteringsprocessen.

Objektsledare/objektspecialisten ska dokumentera brandväggarnas utformning och konfiguration.

Objektägare Teknisk plattform ska besluta och ta fram underlag för brandväggen när det gäller:

- Vad som ska loggas
- Vem som ansvarar för uppföljningen av loggarna.
- Hur ofta uppföljning ska ske.
- Hur länge loggarna ska sparas.

Objektägare-IT beslutar om:

- Vad som är tillåtet för anslutningar mellan säkerhetsdomäner.
- Anslutning av utrustning till interna och externa nätverk.
- Anslutning av externa nätverk till organisationens eget nät med ingående säkerhetsfunktioner, autentisering etc. Beslut dokumenteras.
- Anslutning av trådlösa nätanläggningar.
- Säkerhetsarkitekturer för interna och externa nät samt kommunikationssystem

6.4 Mobil datoranvändning och distansarbete

Objektledare/objektspecialist beslutar om ett verksamhetssystems information får bearbetas på distans med stationär eller mobil utrustning

Vid distansarbete i verksamhetssystem ska endast Ale kommuns datorer med DA-uppkoppling få nyttjas som medger en säker autentisering av användaren.

Kraven på teknisk säkerhet och praktisk hantering av mobil utrustning finns dokumenterad i informationssäkerhetsinstruktion Användare.

6.5 Styrning av åtkomst för extern leverantör

Extern anslutning för extern leverantör till tjänster i Ale kommuns nät ska

- ske med en säkerhetsnivå som motsvarar intern anslutning.
- godkännas av objektledare/objektspecialist som tillsammans med IT-avdelningen ser över vilken autentiseringsmetod samt vilka tekniska lösningar som behövs.
- vara möjligt att i efterhand följa upp i fråga om vem som kopplat upp sig, vid vilken tidpunkt och vilka resurser som utnyttjats

Objektledare/objektspecialist

- beslutar och godkänner åtkomsträttigheter till endast information, program eller delar av operativsystemet som krävs för att kunna utföra uppdraget.
- uppdaterar systemsäkerhetsplanen enligt de beslut som har tagits avseende extern anslutning för extern leverantör.

7 Anskaffning, utveckling, underhåll och avveckling av informationstillgångar

All förändring hanteras enligt gällande förändringsprocess som beskrivs i avsnitt 5.3.

7.1 Säkerhetskrav på verksamhetssystem

Verksamhetssystem som tas i bruk ska ha stämts av mot de säkerhetskrav som verksamheten och Ale kommuns arkitektur för infrastrukturen ställer.

En systemsäkerhetsanalys ska upprättas för varje verksamhetssystem. Objektsledare ansvarar för att fastställa och dokumentera systemsäkerhetsanalysen.

Systemsäkerhetsanalysen avser att ett verksamhetssystem redovisar väsentlig information och de samlade kraven på systemet. Det ska framgå vilka säkerhetsåtgärder som är vidtagna samt de eventuella ytterligare säkerhetsåtgärder som behöver vidtas för att kraven på verksamhetssystemet ska uppfyllas.

Som verktyg för systemsäkerhetsanalys ska Ale kommuns systemsäkerhetsplan användas som är utformad enligt gällande krav.

7.1.1 Hantering av datamedia

Känslig information lagrad på datamedia såsom hårddisk, ska hanteras och förvaras på ett sådant sätt att den inte kan läsas av obehörig.

IT-chef ska fatta beslut om hur:

- Datamedia med verksamhetssystemets information ska kasseras.
- Datamedia med sekretessbelagd information ska kasseras.

7.2 Säkerhet vid anskaffning av informationstillgångar

Vid anskaffning av informationstillgångar ska Ale kommuns upphandlingsregelverk och Ale kommuns arkitekturdokument följas.

7.2.1 Kontroll av utomstående tjänsteleverantör

Objektägare ansvarar för att

- Vid upphandling av nya eller förändring av nuvarande system kontakt tas med IT-avdelningen för att stämma av att kraven stämmer överens med kommunens krav och IT-miljö.
- Vid avtalsskrivande med ny utomstående leverantör ska beaktas hur leverantören följer aktuell lagstiftning och säkerhetsföreskrifter som gäller inom kommunen.
- Beställaren av tjänsten och tecknare av leverantörsavtal ansvarar för att leverantören i samband med avtalsskrivande undertecknar en ansvarsförbindelse för bolag och ett sekretessavtal.
- Beställare ansvarar för att följa upp och granska leverantörens tjänster vid förändringar i deras uppdrag. I dessa fall ska en förnyad bedömning av risker göras.

- Intentionen i Förvaltningsmodell-IT följs.

7.3 Säkerhet i utvecklings- och underhållsprocesser

Objektsledaren/objektsspecialisten ansvarar för

- systemunderhåll och fattar beslut om hur programändringar ska utföras innan förändring genomförs.
- beslut om tidpunkt för installation av nya programversioner.
- att berörda användare kontaktas vid eventuella störningar eller avbrott under installation eller vid förändring av program.
- att all systemdokumentation inklusive utveckling och förändringar i verksamhetssystemet dokumenteras.

För systemdokumentationen gäller att:

- En kopia av systemdokumentationen i sin helhet ska förvaras väl skild från originalet.
- Dokumentationen ska endast vara åtkomlig för behörig personal.
- Den ska i rimlig omfattning och grad vara fullständig och aktuell samt uppdateras vid förändringar i verksamhetssystem.

7.4 Avveckling av informationstillgångar

7.4.1 Avveckling av informationstillgång ska godkännas av objektsägare som även ansvarar för att:

- uppsägning av tillhörande avtal sker
- servicekonton avbeställs
- kommunikationslösningar med externa leverantörer sägs upp
- regler för hur informationen ska arkiveras även regleras av dokumenthanteringsplaner och gallringsbeslut
- en beställning skickas till IT-avdelningen för avstängning av informationstillgången samt hur avvecklingen ske

7.4.2 Avveckling av utrustning

Verksamhetssystem, nätverksutrustning och lagringsmedia som innehåller känslig information eller licensierade program ska förstöras, avmagnetiseras eller överskrivas på ett säkert sätt.

8 Rapportering av säkerhetshändelser och brister

8.1 Hantering av informationssäkerhetshändelser och förbättringar

En informationssäkerhetshändelse är en oönskad, negativ händelse för kommunens information.

8.1.1 Händelse

En informationssäkerhetshändelse kan vara att informationen inte är tillgänglig, har tagits bort eller förvanskats genom:

- Att tjänster, funktioner, utrustning eller andra resurser inte fungerar som de ska.
- Systemfel eller överbelastning
- Misstag
- Försummelse när det gäller att följa policies eller rutiner.
- Någon har tagit sig in i system som man inte har behörighet till.

8.1.2 Incident

En informationssäkerhetsincident påverkar eller kan komma att påverka kommunen negativt när det gäller konfidentialitet, tillgänglighet, spårbarhet och riktighet.

En informationssäkerhetsincident kan uppstå genom att:

- Obehöriga får tillgång till kommunens information (sekretess)
- Kommunens verksamhetssystem inte är tillgängliga på avsett vis (tillgänglighet)
- Kommunens information är oriktig, förvanskad eller ofullständig (riktighet)

8.1.3 Uppföljning

Uppföljning av informationssäkerhetshändelser, funktionsfel, misstanke om intrång eller andra störningar ska processbeskrivas av IT-avdelningen.

Processen ska innehålla:

- hur och till vem rapportering ska ske.
- Resurser ska finnas för att prioritera och åtgärda inträffade incidenter/informationssäkerhetshändelser.
- Hur händelser och åtgärder kan följas upp i efterhand.
- Rutiner finnas för återställning till normal drift efter att en informationssäkerhetsincident åtgärdats.

Objektsledaren och objektsledare-IT ska i samarbete upprätta en rutin som omfattar följande.

- Hur användarna informeras vid driftstörningar.
- Hur rapportering ska ske vid störningar, fel och IT-incidenter.
- Agerande vid samtidiga störningar i flera system.
- Hur prioritering ska göras mellan system.

Informstionssäkerhetsarbetet beskrivs mer ingående i avsnitt 2.

9 Kontinuitetsplanering

Dessa ska finnas dokumentarde i Förvaltningsplan IT.

9.1 Generell kontinuitetsplanering

Det ska i händelse av ett avbrott eller kris finnas en kontinuitetsplan för varje sektor/verksamhet. En kontinuitetsplan ska innehålla planer och annan information som behövs om en allvarlig störning skulle inträffa.

Grunden till kontinuitetsplanen utgörs av att verksamheten identifierar sina kritiska processer (huvud- och stödprocesser) samt kritiska resurser i form av personal, verksamhetssystem, el, telefon, reservlösningar, utrustning, material, etc. som krävs för att huvud- och stödprocesser ska fungera.

Baserat på verksamhetens krav på tillgång till kritiska processer, kritiska resurser och genomförda riskanalyser ska kontinuitetsplaner utformas för att hantera en allvarlig störning, avbrott eller kris.

För kontinuitetsplaner som inkluderar verksamhetssystem som en kritisk resurs ska objektsägaren upprätta en överenskommelse med IT-avdelningen gällande längsta tid som information kan vara otillgänglig eller verksamhetssystemet bedöms kunna vara ur funktion innan verksamheten äventyras. Till grund för beslut ligger resultat från genomförda riskanalyser

Objektsägaren ansvarar för att ta fram alternativa manuella rutiner om allvarliga störningar sker.

Vid en allvarlig störning som påverkar flera verksamheter har kommunledningen ansvar för prioriteringen av resurser.

Kontinuitetsplanen ska övas regelbundet och uppdateras vid förändringar för att säkerställa att den är aktuell och ändamålsenlig.

9.2 IT-avdelningens kontinuitetsplanering

Kontinuitetsplan för IT-avdelningen ska finnas framtagen för att oförutsedda störningar ska kunna hanteras.

Kontinuitetsplanen för IT-avdelningen ska innehålla återstarts- och reservrutiner för IT-driften som vidtas inom ramen för ordinarie drift för att verksamhetssystemen ska kunna återstartas inom fastställd tid.

Kontinuitetsplanen ska testas regelbundet och uppdateras vid förändringar. Planerna ska underhållas genom regelbundna granskningar och övningar för att säkerställa att de är aktuella och ändamålsenliga.

I kontinuitetsplanen ska det finnas identifierat vilka system som för verksamheten är mest kritiska och i vilken ordning dessa ska återstartas. En kontinuitetsplan kan till exempel innehålla:

- Scenarier
- Organisation och ledning.

- Systemlista med kritikalitet
- Återstartsrutiner och plan för återstart av system.
- Rutiner för reservdrift och inkoppling av reservkraft.
- Alternativt driftställe.
- Inventarielista och licenser.
- Kontaktuppgifter.
- Hur man ska gå tillväga för att aktivera planen.
- Testplan.
- Krisarbetsplats för åtkomst till serverhall.

10 Skydd av informationstillgångar

10.1 Personuppgifter och register

Objektsägaren ansvarar för att alla personuppgifter som hanteras inom sitt objekt/informationstillgång anmäls till personuppgiftsombudet (fr.om. 25 maj 2017 till Dataskyddsombudet, förkortat ”DSO”). Personregister som behöver upprättas ska som huvudregel upprättas i ett verksamhetssystem. Om detta inte är möjligt ska registret ändå anmälas till ovan nämnda funktioner.

10.2 Efterlevnad av rättsliga krav

IT-avdelningen ansvarar för att licenser årligen uppdateras för att säkerställa att de avser rätt antal licenser, för antal programvaror och operativsystem som är kopplade till förvaltningsobjekt Teknisk plattform och IT-arbetsplats.

Objektsägaren ansvarar för att licenser årligen uppdateras för sina förvaltningsobjekt.

10.3 Kontroll av teknisk efterlevnad

Interna och externa penetrationstester ska göras återkommande.

Penetrationstester på externa kommunikationssystem (Brandvägg etc.) respektive på interna verksamhetssystem ska göras minst årligen och bör utföras av en extern part.

Granskning av loggar (brandvägg, operativsystem med mera) ska göras regelbundet enligt avsnitt 5.7.

10.4 Efterlevnad av policies och riktlinjer för informationssäkerhet

Regelbundna granskningar ska genomföras minst en gång per år och omfatta.

- Riktlinjer och policy för informationssäkerhet.
- Licenser
- Driftsdokumentation
- Loggar
- Verksamhetssystem
- Säkerhetsplan för respektive system
- Lagar