ALE KOMMUN

Informationssäkerhet

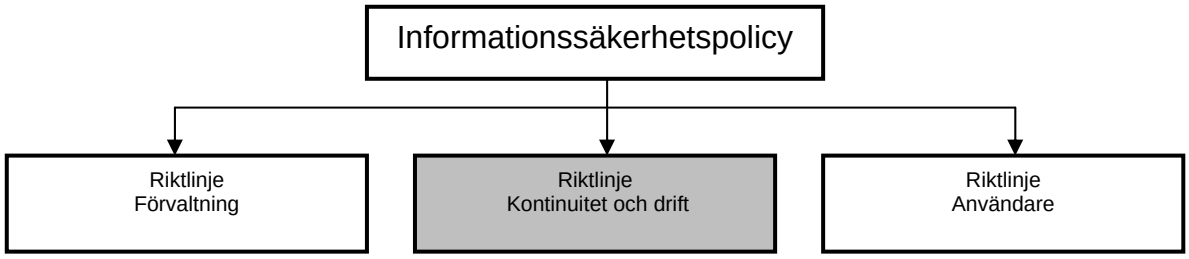
Riktlinje – Kontinuitet och drift

Fastställd av kommundirektören 2011-06-20

Innehåll

1 Informationssäkerhet

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

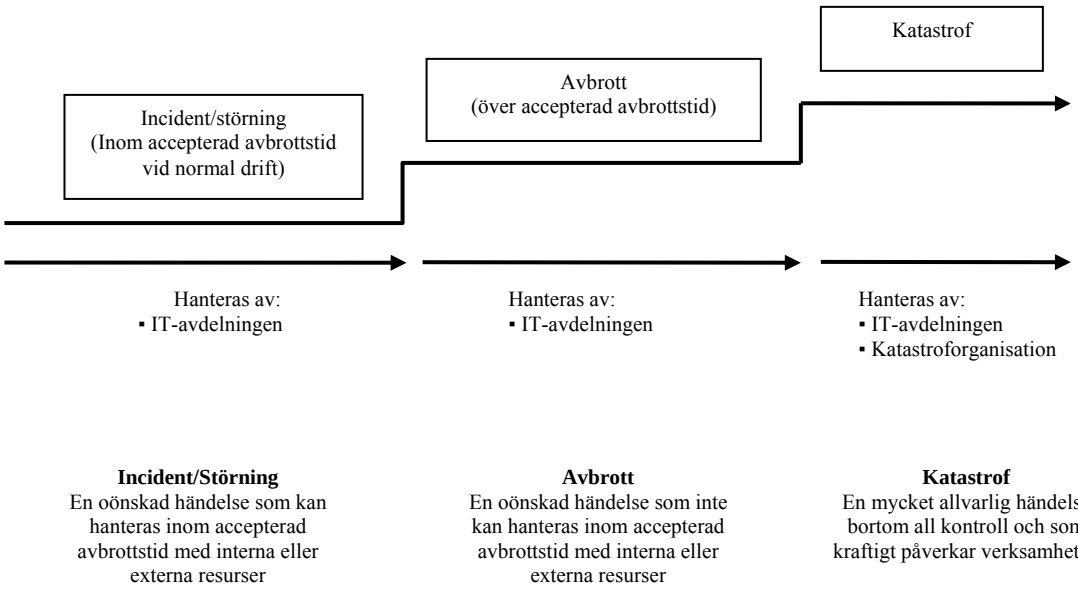


Informationssäkerhetspolicyn redovisar ledningens viljeinriktning och mål för informationssäkerhetsarbetet. Riktlinje Kontinuitet och drift utgår från policyn och syftar till att redovisa:

- driftorganisationen för informationssäkerhetsarbetet
- 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

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



2.1 IT-Support

IT-support är bemannad dagtid och utgör grunden i IT-funktionen.
IT-support 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.

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 (Det ska omfatta enskild användare om

en bedömning görs att felet är av den karaktär som ovan nämns när det gäller image/ekonomiskt.).

3 Hantering av tillgångar

3.1 Ansvar för tillgångar

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

IT-avdelningen ansvarar för att det ska finnas ett register över IT-utrustning (Hårdvara, nätverksutrustning med mera) och programvaror.

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

3.2 Klassificering av information

IT-systemen i Ale kommun ska klassas utifrån den information som hanteras i respektive system. Applikationsansvarig för respektive system ansvarar för att klassningen genomförs.

Klassningen ska genomföras efter Ale kommuns klassningsmodell. Klassningen genomförs utefter aspekterna sekretess, tillgänglighet och riktighet.

Med detta menas:

Sekretess	Information ska skyddas så den inte avsiktligt eller oavsiktligt görs tillgänglig eller avslöjas för obehörig eller kan nyttjas på annat otillåtet sätt.
Tillgänglighet	Informationen ska vara tillgänglig för behöriga användare efter identifierat behov både för interna och externa intressenter.
Riktighet	Information ska vara skyddad mot oavsiktlig och avsiktlig förvanskning.

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.

4 Personalresurser och säkerhet

4.1 Kontroll av utomstående tjänsteleverantör

Vid avtalsskrivande med ny utomstående leverantör ska beaktas hur leverantören kan följa de 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 för att säkerställa att kommunens säkerhetsföreskrifter efterlevs. Vid avtalsskrivande med ny leverantör ska Ale kommuns mallar för ansvarförbindelse för bolag och sekretessavtal användas.

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.

5 Fysisk och miljörelaterad säkerhet

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.

5.1 Säkrade utrymmen

5.1.1 Tillträdesskydd

Endast utsedd och behörig personal har tillgång till serverrum och utrymmen med känslig information. IT-chef ansvarar för vem som ska få tillträde till dessa utrymmen för att kunna utföra sina arbetsuppgifter. Tillträdet ska registreras och dessa uppgifter hanteras i enlighet med gällande rutin.

I utrymmen med känslig information eller för IT-systemets drift viktiga dator- och kommunikationsutrustning ska extern personal som till exempel servicepersonal, städpersonal med flera endast ges tillträde när det är nödvändigt och då under översikt. Besöksmottagaren ansvarar för att extern personal övervakas när behovet föreligger.

5.1.2 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.

5.1.3 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.

5.1.4 Klimatanläggning

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

5.1.5 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 dieselaggregat finns för användande då kommunhuset 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 fastighetsavdelningen på sektor samhällsbyggnad. samhällsplaneringssektorn.

6 Styrning av kommunikation och drift

6.1 Driftdokumentation

Relevant driftdokumentation ska finnas upprättad av IT-avdelningen. All driftdokumentation ska i rimlig omfattning vara fullständig och aktuell samt uppdateras vid förändringar i IT-system.

Kopia av driftdokumentationen ska förvaras skyddad och åtskild från driftstället.

Driftdokumentationen bör minst omfatta:

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

6.2 Säkerhetskopiering och återläsning av data

Applikationsansvarig ska för sitt IT-system besluta i samråd med IT-avdelningen:

- Om vilken information som ska omfattas av säkerhetskopiering
- Om intervallen för kopiering
- Om hur många generationer säkerhetskopior som ska finnas
- hur säkerhetskopior ska förvaras
- Om och när återläsningstester ska genomföras

Backup enligt systemsäkerhetsplan ska redovisas för IT-avdelningen som ansvarar för att säkerhetskopiering av data genomförs på ett säkert och effektivt sätt.

Tester för att återskapa information från säkerhetskopior ska genomföras enligt upprättad plan och resultatet ska dokumenteras.

Regler avseende säkerhetskopiering och återläsning:

- Återställning av data ska kunna ske från valfri dag en månad tillbaka i tiden efter begäran från enskild användare via IT-support. Data ska även kunna återställas från valfritt månadsskifte 12 månader tillbaka i tiden.
- För de system som har teknik för mer aktuell återställning (till exempel transaktions-loggning) sparas i två veckor för Notes, SQL och Oracle (transaktionsloggarna backas upp en gång per dag).
- Säkerhetskopiering ska kunna ske med annat schema för vissa av kommunens verksamhetssystem/verksamheter än ovan efter särskild överenskommelse mellan parterna.

- Säkerhetskopior ska förvaras säkert och brandskyddat på annan geografisk plats än källdata.

Om ingen av dessa nivåer är tillräcklig i förhållande till applikationsansvariges krav ska en skräddarsydd lösning erbjudas.

6.3 Hantering av datamedia

Känslig information lagrad på datamedia såsom hårddisk, cd-skivor, minneskort, ska hanteras och förvaras på ett sådant sätt att den inte kan läsas av obehörig. IT-chef ansvarar för att fastställa vilken information lagrad på datamedia som ska omfattas av särskilda förvaringsrutiner beroende på informationsklassning. Dessa datamedia ska förvaras i utrymmen som är konstruerade för ändamålet.

IT-chef ska fatta beslut om hur:

- Datamedia med IT-systemets information ska kasseras.
- Datamedia med sekretessbelagd information ska kasseras.

6.4 Ändringshantering

Förändringar i driftmiljö, utrustning och rutiner ska ske genom en formell rutin som innebär:

- Identifiering och registrering av större ändringar
- Konsekvensanalys av sådana ändringar
- Godkännande/beslutsform för ändringar
- 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.

6.5 Skydd mot skadlig kod

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

Säkerhetspatchar till operativsystem (till exempel MS Windows, Linux med mera) ska installeras snarast eller inom 2 veckor från utgivning. Kritiska säkerhetspatchar ska installeras omgående i samråd med IT-chef.

En process för hantering av ”patchar” ska finnas och vara dokumenterad.

Viruskontroll ska ske automatiskt. Virusdefinitionsfiler ska automatiskt uppdateras löpande för att garantera aktuellt skydd.

6.6 Avveckling av utrustning

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

6.7 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.
En lista på samtliga IT-system/nätverksutrustning som övervakas och på vad som övervakas med avseende på prestanda ska finnas.

6.8 Loggning och spårbarhet

Loggning av aktivitet i IT-system 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 är oskyldiga, samt vem/vilka som antingen har gjort något otillåtet eller begått ett misstag. Med hänsyn till Personuppgiftslagen (PuL) ska loggning begränsas i tid.

Vilka system som övervakas ska finnas dokumenterat.

Följande revisionsloggar för säkerhetsrelevanta händelser ska finnas som minst registrerar:

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

Det ska finnas administratörs- och operatörsloggar som minst registrerar:

- Konto och involverad administratör/operatör
- Start- och sluttid för drift av system
- Vilka processer som involveras
- Datum och tidpunkt för in- och utloggning
- Lyckade och misslyckade försök till åtkomst
- Namnet på den person som för in uppgift i loggen vid manuell loggning

I de fall administratörs-/operatörsåtgärder inte möjliga att logga automatiskt ska manuell logg föras.

Vid uppföljning av säkerhetshändelser via loggar är det mycket viktigt att datorklockor är synkroniserade.

Samtliga loggar ska granskas regelbundet enligt systemsäkerhetsplanen, där det ska framgå vad som ska loggas, hur ofta loggarna ska granskas, vem som ska utföra granskningen samt vad som är att betrakta som överträdelse. Vidare ska beslut finnas för hur överträdelser ska hanteras. Detta görs i samråd med applikationsansvarig.

Loggarna ska lagras på säker plats och sparas så länge som det anses nödvändigt.
Loggar som kan vara integritetskänsliga får endast sparas i 7 dagar. Därefter ska loggarna raderas.

6.9 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 åtskildaproduktions-, utvecklings- och testmiljöer, vilket minskar risken för att utvecklings- och testarbete stör produktionen.

Sammankoppling av nätverk får endast ske efter att säkerhetsaspekterna analyserats och nödvändiga skyddsåtgärder vidtagits av respektive nätverks systemförvaltare.
I samband med att information överförs genom data- och telekommunikation, uppkommer risker för avlyssning och förändring av den överförda informationen.

Respektive IT-systems applikationsansvarig 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.

6.10 Drift- och övervakningssystem

Ett övervakningssystem för övervakning av nätverksenheter såsom servrar, routrar och skrivare ska finnas för att åtgärda driftstörningar innan det blir ett problem för användarna.
Rutin för gällande övervakningssystem ska finnas dokumenterad.

6.11 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.

7 Styrning av åtkomst

7.1 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.

Behörighet som upphört att gälla ska spärras inom 5 arbetsdagar. Minst en gång per år ska det kontrolleras att endast behöriga personer är registrerade i behörighetssystemet för IT-systemet.

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.

7.2 Styrning av åtkomst till nätverk

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

IT-avdelningen beslutar:

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

IT-avdelningen ska klarlägga säkerhetsarkitekturer för interna och externa nät samt kommunikationssystem.

IT-chef 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. ska dokumenteras.
- Anslutning av trådlösa nätanläggningar.
- Säkerhet vid internetanslutning.

8 Rapportering av säkerhetshändelser och svagheter

8.1 Hantering av informationssäkerhetshändelser och förbättringar

En informationssäkerhetshändelse är en oönskad, negativ händelse för kommunens information och IT-system, som till exempel att informationen inte är tillgänglig, har tagits bort eller förvanskats. En informationssäkerhetsincident påverkar eller kan komma att påverka kommunen negativt när det gäller sekretess, tillgänglighet och riktighet.

Exempel på informationssäkerhetshändelse kan vara:

- 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.

En informationssäkerhetsincident kan uppstå genom att exempelvis:

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

Process för hur uppföljning av informationssäkerhetshändelser, funktionsfel, misstanke om intrång eller vid andra störningar ska utformas av IT-avdelningen.

I en process för incidenthantering/informationssäkerhetshändelser ska:

- Det vara klarlagt hur och till vem rapportering ska ske.
- Resurser finnas för att prioritera och åtgärda inträffade incidenter/informationssäkerhetshändelser.
- Händelser och åtgärder vara möjliga att följa upp i efterhand.
- Rutiner finnas för återställning till normal drift efter att en informationssäkerhetsincident åtgärdats.
- 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.

9 Kontinuitetsplanering

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

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

Kontinuitetsplanen för IT-avdelningen ska innehålla återstarts- och reservrutiner för IT-driften som vidtas inom ramen för ordinarie drift för att IT-systemen 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 datorhall.

10 Efterlevnad

10.1 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 IT-infrastrukturen.

10.2 Kontroll av teknisk efterlevnad

Interna och externa penetrationstester ska göras återkommande.

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

Granskning av loggar (brandvägg, operativsystem med mera) ska göras regelbundet

10.3 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