MORA KOMMUN

RIKTLINJER IT-SÄKERHET

Dokumentbeskrivningar

Policy
En policy ska ange viljeinriktningen för ett specifikt område. Den ska vara vägledande för beslut och styrning. En policy som är av principiell beskaffenhet eller av större vikt ska beslutas av kommunfullmäktige och i övrigt av kommunstyrelsen. En policy gäller tills vidare och bör därför revideras vart fjärde år och följa mandatperioden.

Program och planer
Ett program anger långsiktiga avsikter i en fråga av större vikt. Ett program är mer beskrivande än en policy och mer övergripande än en plan. Om program ska gälla för hela kommunen ska den antas av kommunfullmäktige.

En plan eller handlingsplan innehåller åtgärder som ska vidtas inom ett särskilt område och syftar till att förverkliga exempelvis mål, policy, lagar mm. En handlingsplan är mer konkret och specifik än en plan och innehåller exempelvis ansvar. De bör revideras vart fjärde år och följa mandatperioden

Föreskrifter
Regeringen har i förordningar gett kommunerna rätt att utfärda lokala föreskrifter med mer detaljerade bestämmelser än i förordning.

Riktlinjer och rutinbeskrivningar
En riktlinje innehåller anvisningar om hur en fråga ska hanteras. Den är vägledande i hur tjänstemän bör agera.

Reglemente
Kommunfullmäktige beslutar hur kommunen ska organiseras och vilka nämnder som skall finnas och hur de skall vara sammansatta. Det är obligatoriskt för kommunfullmäktige att utfärda reglementen för nämnderna. Reglementen är ett regelverk om nämndernas arbetsformer och har till uppgift dels att klargöra befogenhetsfördelningen mellan de olika nämnderna. Kommunfullmäktige beslutar också om sitt eget reglemente s.k. arbetsordning samt revisionens.

Bolagsordning och ägardirektiv
För de kommunala bolagen motsvaras reglementena av bolagsordning och ägardirektiv. Dessa kommunala aktiebolag ska följa såväl aktiebolagslagen som delar av kommunallagen.

Stadgar
Ett äldre begrepp för riktlinjer är stadgar, vilka antas av fullmäktige. Stadgar används mest i formen av regler för hur en förening eller stiftelse ska arbeta.

Taxor och avgifter
Kommunen har så kallad avgiftsmakt det vill säga befogenhet att ta ut avgifter av enskilda som ersättning antigen för kommunala prestationer eller för rätten att nyttja allmänna platser och inrättningar. Avgift som är privaträttsliga och är grundade på frivilliga avtal kallas avgifter. Avgifter som är offentligrättsliga det vill säga påtvingad prestation med stöd av bestämmelser i en allmän författning kallas taxor. Taxor och avgifter beslutas av fullmäktige.

Arvoden och andra kommunala stöd
Fullmäktige får besluta att förtroendevalda i skälig omfattning får ersättning för sitt uppdrag och därtill uppkomna omkostnader.

Kommunen har möjlighet att ge olika stöd exempelvis till föreningar.

Riktlinjer IT-säkerhet

Fastställd	Kommunstyrelsen Mora 2020-04-07 § 121 Kommunstyrelsen Orsa 2019-10-28 § 134 Kommunstyrelsen Älvdalen 2020-02-11 § 31
Reviderad	-
Produktion	Kommunstyrelseförvaltningen
Dnr	2018/00434 030

Innehållsförteckning

1 Inledning

IT är en del av vår vardag som underlättar för oss. Informationstillgångarna som finns i IT-komponenter måste skyddas så att de inte hamnar i orätta händer, förvanskas eller förstörs då det kan få stora konsekvenser tex ekonomisk förlust, felaktiga beslut som leder till personligt lidande, skadat förtroende för kommunen, felbehandling av patienter, reprimander från myndigheter och så vidare.

Det är viktigt att IT-säkerheten är tillräckligt hög för att bemöta aktuell hotbild, att användarna har hög kunskap om IT-säkerhet och att det finns rutiner för att hantera IT-säkerhetsincidenter och förändringar i IT-miljön så att inga säkerhetsluckor uppstår.

1.1 Vad är IT-säkerhet

IT-säkerhet är en del av informationssäkerhet. Administrativ säkerhet och fysisk säkerhet är också en del av informationssäkerhet.

Informationssäkerhet
Informationssäkerhet innefattar att skapa och upprätthålla lämpliga rutiner och skydd av information gällande:

- Konfidentialitet, att information inte tillgängliggörs eller avslöjas för obehörig
- Riktighet, att informationen är korrekt, aktuell och fullständig
- Tillgänglighet, att informationen är åtkomlig och användbar av behörig

Informationssäkerhet omfattar information i olika former oavsett hur informationen lagras, bearbetas och kommuniceras. Information kan tex vara text, film och bilder som hanteras med stöd av IT, papper eller direkt av människor i tal.

IT-säkerhet
IT-säkerhet är säkerhet i IT-komponenter för att uppnå och upprätthålla informationssäkerhet. IT-säkerhet koncentrerar sig på hot och skydd förenade med användning av IT-komponenter. IT-säkerhet handlar om att förstå risker och hotbilden, hantera sannolikheter för skada samt att balansera kostnader för IT-säkerhetsskydd mot värdet av det som skyddas.

Informationsklassning är grunden till att kunna ställa krav på IT-säkerhet. Skyddsåtgärder gällande IT-säkerhet kopplas sedan till informationsklasserna. Olika typer av åtgärder används för att uppfylla kraven.

Fysisk och miljörelaterad säkerhet
Fysisk och miljörelaterad säkerhet avser att förhindra otillåten fysisk åtkomst, skador på och störningar i IT-komponenter. Exempel; lås, larm, övervakning, passagesystem, brandlarm, släckanläggningar, reservkraft, UPS etc.

Administrativ säkerhet
Administrativ säkerhet avser hur den administrativa delen sköts, tex riktlinjer, rutiner, instruktioner samt lagar.

1.2 Begrepp

Begrepp	Definition
Autentisering	Identitetskontroll, kontroll av att någon är den de utger sig för att vara. Kan vara en person eller IT-komponent.
Behörighet	Tilldelad rättighet att använda informationstillgång på ett specificerat sätt.
Informationsklassning	Metod för att värdera och prioritera information efter krav på konfidentialitet, riktighet och tillgänglighet. Information klassas i olika nivåer beroende på skyddskrav.
Informationssäkerhet	Konfidentialitet, riktighet och tillgänglighet hos information. Skydd av informationstillgångar syftande till att upprätthålla önskad konfidentialitet, riktighet och tillgänglighet
IT-komponent	IT-baserad komponent, tex IT-system, applikationer, stödsystem, servrar, databaser, infrastruktur och operativsystem med tillhörande dokumentation
IT-nära	Den del av objektområde som överlappar IT-verksamheten benämns IT-nära. Fokus är på IT och teknik samt kravställa och koordinera interna och externa IT-leverantörer.
IT-säkerhet	IT-säkerhet är säkerhet i IT-komponenter för att uppnå och upprätthålla informationssäkerhet
Konfidentialitet	Att information inte tillgängliggörs eller avslöjas för obehörig.
MOA	Mora, Orsa och Älvdalens kommuner och dess kommunala bolag.
Riktighet	Att informationen är korrekt, aktuell och fullständig.
Spårbarhet	Aktiviteter utförda i IT-system ska kunna härledas till en identifierad användare vanligtvis via olika loggar
Tillgänglighet	Att informationen är åtkomlig och användbar av behörig.

2 Roller och Ansvar

Kommunfullmäktige, kommunstyrelse och nämnder samt kommunala bolagsstyrelser har det yttersta ansvaret för IT-säkerhet i den verksamhet som bedrivs inom sina respektive verksamhetsområden.

Ansvaret för IT-säkerhet följer verksamhetsansvaret, verksamheten har ansvar för sin IT-säkerhet och ställer krav på IT-enheten samt externa leverantörer. De som arbetar specifikt med IT-säkerhet fungerar som stöd till verksamheter för att de ska kunna fullfölja sitt ansvar för IT-säkerheten.

IT-säkerhetsarbetet ska bedrivas systematiskt vilket innebär att upprätta, införa, driva, övervaka, granska, underhålla och förbättra IT-säkerheten. Eftersom världen är i ständig förändring måste IT-säkerhetsarbetet ständigt anpassas till nya lagar, nya hotbilder och strömningar i samhället.

2.1 Verksamhetsansvarig

Verksamhetsansvariga ansvarar för IT-säkerhet inom sin verksamhet. Verksamhetsansvarig ska se till att användare följer riktlinjer, processer, rutiner, har IT-säkerhetsmedvetande och tillräcklig förståelse samt kunskap för att IT-säkerhet kan uppnås i verksamheten. Verksamhetsansvarig ansvarar även för att vid behov aktivera avbrottsplaner.

2.2 Användare

Användare ansvarar för att följa riktlinjer, processer, rutiner gällande IT-säkerhet. Användare har skyldighet att rapportera IT-säkerhetsrelaterade brister och incidenter till Service Desk samt till närmaste chef.

2.3 IT-enhetens ansvar

IT-enheten ansvarar för att:

- IT-säkerhetsriktlinjer samt att dokumentation gällande detta är tillgänglig och aktuell.
- IT-säkerheten i IT-miljö är tillräcklig och uppfyller verksamhetens krav och legala krav.
- Leverera tjänster inom IT-säkerhet samt övervaka aktuell och beslutad IT-säkerhet.
- Rapportera och följa upp IT-säkerhetsfrågor och rapportera avvikelser och incidenter till nämnden.
- Ha en utsedd IT-säkerhetsansvarig

2.4 IT-säkerhetsansvarig

IT-säkerhetsansvarig ansvarar för att kravställa, stödja och kontrollera arbetet med att nå och upprätthålla rätt nivåer av IT-säkerhet. IT-säkerhetsansvarige ska samverka med Informationssäkerhetssamordnaren. IT-säkerhetsansvarige ska:

- Utforma och förvalta riktlinjer och instruktioner för IT-säkerhet
- Stödja verksamheter i IT-säkerhetsfrågor
- Följa upp och granska efterlevnaden av riktlinjer och instruktioner
- Stödja i framtagning och genomförande av handlingsplaner för att åtgärda brister som konstaterats i samband med IT-säkerhetsgranskningar eller riskanalyser
- Bistå vid utredning av misstänkta och inträffade IT-säkerhetsincidenter
- Stödja verksamheter vid extern kravställning rörande IT-säkerhet och uppföljning av externa leverantörers säkerhetsåtaganden
- Stödja i verksamheters riskanalyser rörande IT-relaterade risker
- Verka för höjande av säkerhetsmedvetande inom IT
- Ta fram statusrapporter för kommunens IT-säkerhet
- Omvärldsbevaka
- Nätverka, samverka externt inom området

2.5 Objektägare och Objektägare IT

Objektägare ansvarar för att objektet efterlever IT-säkerhetsriktlinjer. Objektägaren är ansvarig för att informationsklassning av objektet sker samt tilldela resurser så att informationsklassningsnivån kan uppnås.

Objektägare IT ansvarar för att IT-komponenter ges ett IT-säkerhetsskydd som motiveras av klassningen av system genom hela dess livscykel, införande, drift och avveckling.

Objektägare och Objektägare IT beslutar om IT-säkerhetsrelaterade mål för objekt. Vid avveckling av IT-komponenter ansvarar Objektägare och Objektägare IT för att en plan upprättas gällande hur information ska migreras, raderas eller slutarkiveras.

2.6 Objektledare och Objektledare IT

Objektledaren och objektledare IT samverkar för att IT-säkerhetsrelaterade mål uppnås och beslutade åtgärder genomförs.

2.7 Objektspecialist/Superanvändare

Objektspecialist/Superanvändare ansvarar för att utföra IT-säkerhetsrelaterade aktiviteter på uppdrag av objektledare.

2.8 IT-specialist

IT-specialister ansvarar för att utföra IT-säkerhetsrelaterade aktiviteter på uppdrag av objektledare IT, IT-säkerhetsansvarig eller IT-chef.

2.9 Projektägare och styrgrupp

Projektägare och styrgrupp ansvarar för att IT-säkerhetsfrågorna hanteras i projekt.

2.10 Projektledare

Projektledaren ansvarar för att IT-säkerhetsaktiviteter löpande planeras och genomförs i projektarbetet.

3 IT-säkerhet för användare

3.1 IT-säkerhetsincidenter

Alla användare har skyldighet att rapportera IT-säkerhetsincidenter och brister. Användare och deltagare i verksamheten som har upptäckt en IT-säkerhetsincident eller svaghet där brott misstänks föreligga, ska inte själva försöka bevisa detta då det kan försvåra utredningar.

3.2 Lösenord

För att logga in i de flesta system används användarnamn och lösenord samt ibland även ytterligare lösningar. Lösenord är personliga och får inte göras kända för andra. Lösenord ska vara ”starkt”, svårt för någon annan att gissa. Det ska inte kunna förknippas med dig som person och ska ha en viss längd och komplexitet.

Hur lösenord ska hanteras av användare ska förtydligas i instruktion för användare.

3.3 Skydd av utrustning

Användning av utrustning ska ske i enlighet med de instruktioner som gäller för användare t.ex. säkerställa att utrustning antingen övervakas eller låses in för att minska risken för stöld. Förlust av utrustning ska direkt anmälas till Service Desk och sedan görs en polisanmälan Utrustning som inte ska användas av nuvarande användare ska alltid lämnas till Service Desk innan utrustningen kan ges till nästa användare. Utrustningen ska vårdas enligt tillverkarens föreskrifter, tex skyddas mot värme och fukt.

3.4 Skadlig kod

Med skadlig kod avses oönskade datorprogram som virus, trojaner, spionprogram och maskar. Dessa kan installeras på en dator eller nätverk utan administratörens vetskap. De stör IT-system, samlar in information eller utnyttjar datorkraft eller minneskapacitet i IT-komponenter.

Hur en användare ska agera vid misstanke om skadlig kod ska förtydligas i instruktion för användare. Användare får inte installera datorprogram själva.

3.5 Lagring och säkerhetskopiering

Information ska lagras på ett säkert sätt. Detta för att informationen ska säkerhetskopieras och kunna återskapas vid händelse av diskkrasch, oavsiktlig radering eller liknande händelser. I instruktion för användare beskrivs hur detta ska ske.

4 IT-säkerhet i objekt

Det finns en beslutad modell för styrning av objekt, det här kapitlet kompletterar denna med riktlinjer gällande IT-säkerhet.

IT- säkerhet ska vara en naturlig del i styrning av objekt. IT-säkerhetsförhållanden ska vara dokumenterade i systemsäkerhetsbeskrivningar och planerade säkerhetsåtgärder ska ingå i objektplaner så att de formellt fastställs och objektägare och har en budget. Målen kan ha sin härkomst och motiveras från tex riskanalyser, revisioner, inträffade incidenter eller krav i dessa riktlinjer.

4.1 Informationsklassning

Informationsklassning innebär att information klassas i olika nivåer beroende på skyddskrav. Detta har till syfte att identifiera känslig och kritisk information så att denna får tillräckligt med IT-säkerhetsskydd samt att undvika överskydd med höga kostnader som följd. Vid osäkerhet är det bättre att ”överklassad”.

4.2 Systemsäkerhetsbeskrivning

Objektets IT-säkerhetsförhållanden ska dokumenteras i systemsäkerhetsbeskrivningar. En systemsäkerhetsbeskrivning ska finnas för varje system.

Av systemsäkerhetsbeskrivningen ska det framgå:

- Vilka informationsmängder som hanteras i systemet och hur dessa är klassade[1]
- Hur systemet är klassat[2]
- Hur behörighetshantering och loggning går till
- Användarinstruktioner med inriktning på säkerhet
- Planerade och genomförda riskanalyser och resultat från dessa
- Vilken kontinuitetshantering som finns

4.3 Behörighetshantering

Behörigheter innebär vissa rättigheter att använda en informationstillgång som finns i tex ett system på ett specifikt sätt. Behörigheter (åtkomsträttigheter) bestämmer vad en användare har rätt att utföra tex. Läsa, söka, skriva, skapa etc.

För att skydda informationen mot obehörig åtkomst behöver användare ange en identitet som kan autentiseras (verifieras), tex. användar-ID och lösenord. Behörighet ska baseras på vilken information användare behöver för att utföra sina arbetsuppgifter. Olika roller som använder ett system kan ha olika behov av information och ska ha olika behörigheter (åtkomstprofiler).

Inom vissa områden tex vård och omsorg behöver man ha behörighet till mycket information i vissa situationer. I dessa fall ska regelstyrd åtkomstkontroll tillämpas. Det ska vara regler som reglerar att man endast får ta del av information som behövs för arbetsuppgifterna. Reglerna måste kompletteras med uppföljning, övervakning och loggning.

För verksamhetssystem är det objektägare eller objektledare i verksamheten som beslutar vilka som ska få tillgång till systemet och vilka behörigheter dessa ska ha. För externa användare ska även tidsbegränsning av behörighet finnas samt sekretessavtal undertecknas.

Det ska finnas en process och rutiner som underhåller och förvaltar behörigheter för ett system. Det gäller till exempel hantering av beställning, ändring, borttagning av behörigheter och rättigheter samt revisioner.

4.4 Logghantering

För att erhålla spårbarhet, möjliggöra IT-säkerhetsincidentutredningar och upptäcka avvikelser från legala och interna regelverk bör system övervakas och loggas avseende användaraktiviteter, avvikelser och fel. Detta är obligatoriskt för system som hanterar information med höga skyddskrav eller om regelstyrd behörighetshantering tillämpas.

---

[1] Informationssäkerhetsriktlinjer styr hur detta ska genomföras

[2] Informationssäkerhetsriktlinjer styr hur detta ska genomföras

Då loggning används ska det finnas processer och rutiner för dess hantering, de ska innefatta hur loggning går till, hur loggar skyddas mot manipulation och obehörig åtkomst, hur länge se sparas och hur de granskas. Processer och rutiner för loggning ska följas upp och dokumenteras.

4.5 Ändringshantering

Ändringar i system ska ske enligt beskrivningar i styrning av objekt och i samordning med förändringsprocessen som används inom IT-nära. Detta innebär att ändringar sker strukturerat för att säkra systemets säkerhet, funktionalitet och användarbarhet samt att minimera antalet fel orsakade av ändringen. Större förändringar i eller omkring ett system ska föregås av en riskanalys.

4.6 Riskanalyser

Risker är tänkbara oönskade händelser som kan inträffa och har en negativ inverkan på system och dess information. En risk är en kombination av hur sannolikt det är att en händelse inträffar och vilken konsekvens det blir. Metod som ska användas för riskanalys ska finnas.

För alla objekt ska en eller flera riskanalyser vara genomförda samt att resultatet ska vara dokumenterat. Riskanalysen för objektet och dess IT-komponenter ska årligen genomlysas och eventuellt uppdateras utifrån nya insikter. Vid större ändringar tex systemuppdatering, nyutveckling, ägarbyte av systemleverantör etc. ska en riskanalys genomföras enligt framtagen metod. Riskanalysens resultat ska dokumenteras.

En riskanalys kan resultera i att åtgärder ska genomföras, dessa ska införas i objektplanen, antigen den för pågående period och/eller kommande period. Projektledaren eller objektledare planerar genomförandet av riskanalysen. Projektägare och objektägare ansvarar för att det blir genomfört.

4.7 IT-säkerhetsincident

Objektägare ansvar för att IT-säkerhetsincidenter, incidenter och allvarliga incidenter relaterade till system rapporteras till Service Desk.

Objektledare ska upprätta avbrottsplaner (del av kontinuitetshantering) att använda vid större avbrott och som ska innehålla ansvarsförhållanden, kontaktpersoner, eskaleringsvägar.

4.8 Kontinuitetshantering

Kontinuitetshantering innebär systematiskt arbete med att och skapa en god återhämtningsförmåga för kritiska verksamhetsprocesser och minimera konsekvenserna av störningar, avbrott och katastrofer. Arbetet innefattar att identifiera kritiska verksamhetsprocesser och dess beroenden av stöd och resurser som t.ex. personal, lokaler och verktyg. Krav på kontinuitet gällande driften av system sker till största delen genom klassning. Höga skyddskrav för tillgänglighet innebär högre krav på säkerhetskopiering och redundans. För objekt med höga skyddskrav måste det finnas en beredskap för hur man hanterar avbrott, avbrottsplaner.

Avbrott kan dock alltid ske oavsett förebyggande IT-säkerhetsåtgärder. Beroende av funktionalitet i system kan vara så högt att system inte kan ligga nere. I dessa fall måste verksamheten ha planer och rutiner för att kunna fullfölja sitt åtagande vem vid systemavbrott.

Efter ett större avbrott ska återgång till normalläge ske så snabbt som möjligt med så små konsekvenser för verksamheten som möjligt, både under och efter avbrottet. Objektägare IT ansvarar för att avbrottsplaner finns på plats och att de motsvarar de krav som finns för objektet.

5 IT-säkerhet i IT-miljön

Detta kapitel innehåller riktlinjer gällande MOAs IT-miljö. IT-säkerhet innefattar säkerhet i tex. system, verktyg och infrastruktur i form av hård- och mjukvara. Gällande infrastruktur och klienter är objekten Teknisk plattform och IT-arbetsplats främst berörda. Kapitlet är strukturerat enligt nedanstående avsnitt i standarden SS-ISO/IEC 27002:2014 som till största delar innehåller säkerhet i IT-miljöer.

Kapitel	Kapitel i 27002
Hantering av tillgångar	8
Styrning av åtkomst	9
Kryptering	10
Fysisk och miljörelaterad säkerhet	11
Driftsäkerhet	12
Kommunikationssäkerhet	13
Anskaffning och utveckling	14
Incidenthantering	16
Granskning och kontroll	18

Standarden innehåller mer vägledning och information än i detta dokument. Standarden kan användas som ett stödjande dokument för att efterleva riktlinjerna.

5.1 Hantering av tillgångar

5.1.1 Identifiering av IT-komponenter och tilldelning av ägare

Alla IT-komponenter ska vara identifierade och ingå i ett objekt. Det ska finnas en förteckning över alla IT-komponenter som underhålls. Rutiner ska finnas för att säkerställa att förteckningen är aktuell. Förteckningen ska skyddas från åtkomst och ändring av obehörig.

5.1.2 Klassning av IT-komponenter

Underliggande IT-komponenter (tex infrastruktur) måste ha minst motsvarande klassning gällande de IT-komponenter (tex verksamhetssystem) som använder dem. Underliggande IT-komponenter kan ibland ges en högre klassning än de verksamhetssystem de stödjer, tex om IT-komponenter stödjer flera system som var för sig inte är kritiska. Beroende på hur IT-komponenter är klassade ska olika säkerhetsåtgärder införas för att uppnå ett tillräckligt bra skydd.

5.1.3 Användarinstruktioner

Regler och instruktioner till hur IT-komponenter får användas ska finnas. Dessa ska baseras på IT-komponenters klassning och skyddskrav. De som använder eller har tillgång till IT-komponenter ska få instruktioner om hur de hanterar dessa resurser, vilka villkor och vilket ansvar som gäller kring den åtkomst de fått sig tilldelad. Regler och instruktioner kan tex. avse användning av:

- Nätverk: t.ex. hur åtkomst till nätverk får ske, hur nätverkstjänster får användas, hur autentisering ska ske och hur utrustning som ansluts till nätverk ska identifieras
- Operativsystem: t.ex. hur åtkomst och autentisering ska ske
- Klientdatorer: t.ex. regler för programinstallationer som utförs av användare

5.2 Styrning av åtkomst

Grundläggande för att skydda information och IT-komponenter är styrning av åtkomst. Behörighetskontrollsystem (BKS) är det samlade systemet för styrning av åtkomst i en (eller flera) IT-komponenter och utgörs vanligen av både tekniska system och administrativa rutiner. Ett BKS omfattar tre säkerhetsåtgärder som tillsammans ska se till att verksamhetens säkerhetsregler (kontinuerligt) följs:

- Identifiering och autentisering av användares uppgivna identitet.
- Reglering av åtkomsträttigheter; vilken information man kommer åt och vad man kan göra med den, t.ex. läsa, skriva, ändra, radera.
- Loggning av användarens aktiviteter.

5.2.1 Identifiering och autentisering

Identifiering innebär att aktiviteter och åtkomst till en IT-komponent kan kopplas till en individ. Alla användar-ID ska vara unika och personliga. Användar-ID och lösenord tillsammans är en möjlighet till autentisering, dvs. verifiering av en uppgiven identitet. Vid åtkomst till information med höga skyddskrav ska stark autentisering användas. Stark autentisering innebär identifiering av en person och verifiering av personens autenticitet genom en kombination av minst två av följande delar:

- Ett lösenord eller någonting annat **som man vet**
- Ett smartkort eller någonting annat **som man har**
- Ett fingeravtryck eller någon annan egenskap **som man är**

Stark autentisering bör tillämpas vid extern åtkomst till MOAs IT-miljö.

Lösenord är alltid konfidentiella och ska skyddas mot åtkomst från andra.

- Rutiner ska finnas som säkerställer att lösenordet skyddas från tex administratörer eller handläggare oavsett hur lösenordet tilldelas, förändras eller återställs.
- Tekniska funktioner ska implementeras där det är möjligt för att kunna följa historik, komplexitet och åldring av lösenord.
- Lösenord ska aldrig skickas i klartext över nätverk. Om det måste ske ska tillfälligt lösenord användas som endast är giltigt för en (1) inloggning.
- Om felaktigt lösenord används mer än definierat antal gånger ska användar-ID låsas i definierad tid och händelsen loggas.

Alla klienter ska förses med låsskärm som automatiskt låser skärmen efter definierad inaktivitet och kan enbart aktiveras igenom förnyad autentisering. Detta för att minska risken för obehörig åtkomst.

5.2.2 Regler av åtkomsträttigheter

Åtkomst till IT-komponenter baseras på dess klassning. Det ställs större krav på metoder för autentisering vid åtkomst till information med höga skyddskrav. Objektägare IT ansvarar för att upprätta ett BKS som motsvarar dessa krav.

Det ska finnas beslutade och dokumenterade regler och rutiner för behörighetshantering, dvs. BKS. Detta inkluderar att underhålla och förvalta behörigheter, exempelvis hantering av beställning, ändring och borttagning av behörigheter och rättigheter. Åtkomst som inte längre behövs eller ny åtkomst som behövs ska åtgärdas snarast inom en arbetsdag. Det ska finnas rutiner kopplade till Norra Dalarnas Löneservice där man säkerställer att reglering av åtkomst sker vid anställning, vid förändring av roll eller arbetsuppgifter samt vid upphörande av anställning.

Gruppidentiteter är inte tillåtna. Om det ska ske ett undantag ska det godkännas av Objektägare och i samråd med informationssäkerhetssamordnare.

Prövning av enskild ska ske och en tystnads- och sekretessförbindelse upprättas innan någon tilldelas åtkomst till IT-komponent med höga skyddskrav. Den enskilde ska utbildas i vad förbindelsen innebär och vilket ansvar som följer. För externa användare tillkommer att

åtkomsttilldelning även ska vara tidsbegränsad och endast gälla för den tiden som behövs för att utföra uppgiften. Berörd chef ansvarar för att detta blir genomfört.

Administrativa åtkomsträttigheter ska vara restriktiva och endast ge de rättigheter som behövs för att utföra sitt uppdrag i den administrativa roll man har.

Uppföljning och revision av samtliga åtkomsträttigheter ska ske regelbundet. Särskild uppmärksamhet kan behöva ägnas då användare med priviligierade åtkomsträttigheter slutar eller byter tjänst. Processer och rutiner för behörighetshantering ska följas upp och dokumenteras.

5.2.3 Säkerhetsloggning

För att erhålla spårbarhet, möjliggöra incidentutredningar och att i efterhand kunna utreda vad som hänt och för att upptäcka avvikelser ska IT-komponenter övervakas och loggas avseende användaraktiviteter, avvikelser, fel och informations-säkerhetshändelser. Loggar ska skyddas mot manipulation och obehörig åtkomst, sparas en viss tid och granskas regelbundet av loggadministratör.

I de fall logginformation går att knyta till en enskild person är de att betrakta som personuppgifter och omfattas då av krav i GDPR. Dessa loggar med personuppgifter ska skyddas från obehöriga. Om loggning används för att tekniskt övervaka ett system av säkerhetsskäl får loggen inte senare användas för andra ändamål/syften. Om kontroller utförs för andra ändamål/syften än det ursprungliga är lagkravet att personen ska informeras och ge sitt samtycke.

5.3 Kryptering

Kryptering innebär omvandling av data för att dölja informationsinnehåll och kan användas för olika ändamål tex. förhindra obehörig åtkomst till information, kryptografiska signaturer garantera informationens riktighet eller äkthet.

IT-enheten tillhandahåller vid behov godkända krypteringslösningar och instruktioner hur dessa ska användas. Informationsklassningen avgör vanligtvis om behov av kryptering föreligger. Då höga skyddskrav förekommer finns ofta behov av kryptering. Krypteringslösningar ska bygga på etablerade standarder som tex. NIST 140-2 eller ISO/IEC 18033. Krypteringslösningar kan medföra risker relaterade till nyckelhantering. Dessa risker behöver hanteras tex. genom:

- Revokering av nycklar möjliggör att avsluta åtkomst till IT-komponenter.
- Validering av nycklars giltighet och autenticitet möjliggör att användare av en IT-komponent kan avgöra om en nyckel är giltig och att innehavaren kan kontrolleras.
- Återställning av nycklar, funktion för att göra det möjligt att återställa information även om nyckel förloras. Detta kan t.ex. åstadkommas genom användandet av en särskild återställningsnyckel eller genom att nycklar säkerhetskopieras.
    - Detta kan innebära andra säkerhetsrisker eftersom nycklarna finns på fler ställen. Det ställer stora krav på åtkomstkontroll, administrativa rutiner och loggning så att åtkomst till nycklar kan spåras.

5.4 Fysisk och miljörelaterad säkerhet

Fysisk och miljörelaterad säkerhet avser att förhindra otillåten fysisk åtkomst, skador på och störningar i IT-komponenter. Informationsklassning ska användas som stöd vid utformande av det fysiska skyddet.

5.4.1 Säkra utrymmen för IT-komponenter

Säkra utrymmen med särskilda säkerhetskrav är serverrum samt korskopplingsutrymmen. Tillträden till säkra utrymmen ska vara restriktiva och endast ges till de personer som behöver tillträde för att utföra sitt uppdrag. Det ska finnas dokumenterat vem som ges tillträde att arbeta i säkra utrymmen. Instruktion för hur arbete i respektive lokal får bedrivas ska finnas. Personer med arbetsuppgifter i säkra utrymmen ska ha god kännedom om de regler som gäller för arbete

dessa lokaler. Säkra utrymmen som innehåller IT-komponenter med höga skyddskrav ska bevakas och fysisk närvaro ska loggas (t.ex. tillträdes- eller videoövervakningsloggar).

5.4.2 Underhåll, reparation och avveckling

Underhåll av utrustning ska ske i enlighet med leverantörens anvisningar.

Reparation av utrustning och IT-komponenter kan kräva åtgärder från extern personal och auktoriserade reparatörer. Sådan personal har oftast varken behörighet till den information som hanteras i IT-komponenten eller tillträde till sådana säkra utrymmen där IT-komponenten finns placerade.

Om underhåll och reparation ska utföras av utomstående på IT-komponent med höga skyddskrav ska alltid sekretessavtal undertecknas. Det kan ibland vara nödvändigt att vidta särskilda åtgärder, t.ex. att känslig information flyttas, raderas eller krypteras innan någon utomstående hanterar utrustningen.

Avveckling av IT-komponenter bör ske på ett sådant sätt att känslig information inte riskerar att komma i orätta händer. Avveckling av IT-komponenter med höga skyddskrav sker genom att information skrivs över i multipla operationer, alternativt att IT-komponenten där informationen lagrats förstörs på ett fullständigt och oåterkalleligt sätt. Krypterad datamedia inte är känslig om nyckel för dekryptering ges ett fortsatt skydd, eller att nyckel destruerats.

5.4.3 Skydd av utrustning

För mobil utrustning är risken för förlust, stöld och skada högre. Mobil utrustning ska förses med stöldskyddsmärkning.

5.4.4 Elförsörjning

Säker elförsörjning (t.ex. avbrottsfri kraft genom UPS och reservkraft) ska finnas så att IT-komponenter skyddas från elavbrott och andra störningar.

5.5 Driftsäkerhet

5.5.1 Driftrutiner

Dokumenterade driftsrutiner ska finnas, vara aktuella och tillgängliga för alla användare som behöver dem. Driftsrutiner ska finnas för väsentliga processer och objekt, såsom:

- Installation och konfiguration av system
- Uppstarts- och nedtagningsrutin
- Säkerhetskopiering
- Underhåll av utrustning
- Supportkontakter vid oväntade funktionella eller tekniska problem
- Hantering av media
- Serverrum

Förändringar i IT-komponenter ska ske enligt beskrivningar i styrning av objekt och i samordning med förändringsprocessen som används inom IT-nära. Denna process ska säkerställa att alla ändringar som införs på tjänster, moduler och komponenter i IT-miljön är riskbedömda, planerade, kommunicerade, testade och godkända.

Utvecklings-, test- och driftmiljöer ska vara separerade för att minska risken för obehörig åtkomst eller ändringar i driftmiljön.

5.5.2 Skydd mot skadlig kod

För att skydda mot skadlig kod behövs metoder för att förebygga, upptäcka skadlig kod och för att återställa IT-miljön efter angrepp. Det räcker inte enbart med tekniskt skydd, det är viktigt att alla som använder IT-komponenter vet hur de kan minska risken att drabbas av skadlig kod samt vad de ska göra om de misstänker angrepp av skadlig kod. IT-komponenter ska skyddas från skadlig kod genom att antivirusprogramvara installeras på klienter och servrar. Skyddet ska regelbundet uppdateras (dagligen). Programvara ska i förebyggande syfte skanna efter skadlig kod i datorer i kommunens nätverk, filer som tas emot via nätverk eller någon form av media och

i webbsidor. IT-komponenter med höga skyddskrav ska regelbundet granskas gällande skaldlig kod.

Uppdatering av system och applikationer ska genomföras löpande för att de ska hållas fria från säkerhetsbrister. Regelmässigt och skyndsamt ska säkerhetspatchar installeras på IT-komponenter enligt tillverkarnas rekommendationer och enligt fastställd rutin.

Om angrepp av skadlig kod inträffat ska det finnas en fastställd rutin för återställning av IT-komponenter. Rutiner för att regelbundet samla in information om skadlig kod, t.ex. prenumerera på nyhetstjänster eller bevaka webbplatser som ger information om ny skadlig kod (t.ex. cert.se) ska finnas.

5.5.3 Säkerhetskopiering

Säkerhetskopiering gällande information, program och speglingar av system är en viktig del av driftsäkerheten. Detta möjliggör återställning av en IT-komponent till ett fungerande tillstånd efter uppkomsten av ett fel, och att åtgärda både riktighet och tillgänglighet hos information. Det är inte alltid möjligt att återställa all information. Sådan information som tillförts systemet efter senaste säkerhetskopiering går normalt inte att återställa.

Spegling ger enbart ett skydd för tillgänglighet och inte riktighet, eftersom informationen är identisk vid spegling vilket innebär att eventuell felaktig information då återfinns på båda ställen.

Genom att fastställa punkterna nedan ska sedan skyddsåtgärder beslutas för alla IT-komponenter.

- Hur stor informationsförlust som kan accepteras för varje IT-komponent (RPO, Recovery Point Objective)
- Längsta acceptabla tiden för att återställa IT-komponenten efter ett avbrott (RTO, Recovery Time Objective)

Säkerhetskopiering och spegling är tillsammans nödvändiga skyddsåtgärder för IT-komponenter med krav på både riktighet och tillgänglighet. Säkerhetskopiering av IT-komponenter med höga skyddskrav gällande höga RTO-krav bör lagras på snabbmedia tex SAN-diskar.

Säkerhetskopiering av IT-komponenter med höga skyddskrav gällande konfidentialitet ska krypteras eller ges motsvarande skydd.

För att skydda från fysiska incidenter och katastrofer som t.ex. brand och översvämning ska säkerhetskopior lagras geografiskt åtskilt från originalmaterialet. Lösningar där man skiljer på långtids- och korttidslagring är enbart långtidslagringen är skild från originalmaterialet. Då bör korttidslagring skyddas genom ett säkert utrymme avsett för datamedia, annars riskerar man att vid en brand förlora all information som tillförts systemet sedan kopiering till långtidslagring skedde, vilket i vissa fall kan vara lång tid.

Säkerhetskopior ska testas regelbundet för att säkerställa att återläsning fungerar som avsett.

5.5.4 Loggning och övervakning

Loggning och övervakning gör det möjligt att upptäcka händelser i IT-komponenter. Genom loggning möjliggörs korrigerande eller förebyggande åtgärder eftersom loggarna kan analyseras. Händelseloggar som registrerar användaraktiviteter, avvikelser, fel och informationssäkerhetshändelser ska skapas, bevaras och granskas regelbundet. Loggar kan innehålla känsliga data och personinformation.

För att kunna använda automatiserade övervakningssystem som är kapabla att skapa konsoliderade rapporter och varningar avseende säkerhet i system och tillämpningar krävs loggning. När loggverktyg samt att alla loggkällor använder gemensam och korrekt tid kan händelser i olika IT-komponenter korreleras. Det ger en bättre och mera heltäckande bild av händelser jämfört med om logg övervakas i varje system för sig.

Loggning ska normalt ske avseende fel och systemhändelser. Loggar ska sparas en förutbestämd tid samt regelbundet analyseras och övervakas. IT-komponentens klassning och objektägarens krav avgör behovet av loggar och övervakningssystem.

Synkronisering av systemklockor ska i relevanta IT-komponenter ske för att säkerställa loggningen av händelser.

5.5.5 Hantering av tekniska sårbarheter

Tekniska sårbarheter i IT-komponenter kan innebära exponering för skadlig kod, dataintrång eller andra sårbarheter. Rutiner ska finnas så att information om tekniska sårbarheter kan erhållas i tid, att sårbarheter kan analyseras och att lämpliga åtgärder kan vidtas.

Om säkerhetspatchning inte är praktiskt möjlig, t.ex. för ”embedded” system eller SCADA-system ska information om tekniska sårbarheter i sådana IT-komponenter inhämtas och analyseras och lämpliga åtgärder vidtas för att hantera den tillhörande risken.

IT-komponenter som exponeras mot Internet ska ske regelbundet och minst en gång per år säkerhetsgranskas så att inga uppenbara sårbarheter exponeras och att tillräcklig säkerhetsnivå upprätthålls. Säkerhetsgranskningen kan till exempel bestå av skanning av sårbarheter med automatiserade verktyg eller så kallade penetrationstester.

Regler för programinstallationer som användare får göra ska finnas. Detta eftersom okontrollerad installation av program kan medföra sårbarheter och incidenter, som exempelvis obehörig åtkomst till information och förlust av riktighet.

5.6 Kommunikationssäkerhet

Kommunikationssäkerhet är skydd i IT-komponent och nätverk som används för datakommunikation i syfte att skydda den information som kommuniceras.

5.6.1 Nätverkssäkerhet

Nätverk ska skydda information i anslutna system och tillämpningar. Klassningen av de objekt och tjänster som använder nätverket styr vilka skyddsåtgärder som ska införas. Skydd för nätverkssäkerhet kan exempelvis vara:

- Autentisering av system
- Kryptering
- Regler för säkerhet och nätverksanslutning
- Begränsning av systemanslutningar
- Brandväggar och intrångsdetekteringssystem
- Loggning och övervakning av nätverk
- Separation av nätverk (segmentering)

Krav gällande skydd av nätverkstjänster ska identifieras, dokumenteras och tillämpas samt inkluderas i avtal för nätverkstjänster om dessa tjänster tillhandahålls som outsourcade tjänster. Teknik för att kryptera och säkra kommunikationen (minst WPA2 PSK) ska alltid användas oavsett skyddskrav.

Segmentering ska tillämpas. Utrustning ska användas för att kontrollera och förhindra obehörig nätverkstrafik mellan olika nätverkssegment.

Brandväggspolicy ska finnas och det ska framgå vilka nätverkstjänster som ska tillåtas, vilka händelser och aktiviteter som ska loggas och följas upp. Brandväggar ska konfigureras enligt brandväggspolicyn. Brandväggar och brandväggspolicyer ska revideras periodiskt.

Kommunikationstjänster med externa nätverk ska dokumenteras och godkännas av Objektägare IT för Teknisk plattform innan inkoppling får ske.

5.7 Anskaffning och utveckling av IT-komponenter

Korrekt IT-säkerhet för IT-komponenter ska säkerställas över hela livscykeln och börjar vid anskaffning eller utveckling.

5.7.1 Säkerhetskrav på IT-komponenter

Krav gällande IT-säkerhet ska vara med vid inskaffande av nya IT-komponenter och förbättringar av befintliga. IT-säkerhetskraven bygger på klassning som tilldelats IT-komponenten. Objektägare IT ansvarar för att rätt tekniska krav formuleras som överensstämmer med verksamhetens krav. Utveckling, anskaffning eller förändring av underliggande IT-komponenter i form av infrastruktur, stödsystem m.m. ska ha minst motsvarande krav som de system som de stöder.

5.7.2 Säkerhetskrav vid upphandling av IT-stöd

Vid upphandling av IT-stöd gäller ovanstående riktlinjer för säkerhetskrav på IT-komponenter. Det är än viktigare vid extern upphandling att vara tydlig när det gäller kravställning av IT-säkerhet. Externa leverantörer använder kanske annan terminologi och tillämpar andra nivåer av klassning och tolkar de olika nivåerna på annat sätt. Leverantören ska delge hur de bedriver IT-säkerhetsarbete i den operativa verksamheten.

I kravspecifikationer ska alltid tydliga krav på IT-säkerhet formuleras och användas vid utvärdering av anbud. Upphandling av IT-stöd ska alltid göras i samverkan med berörd verksamhet, IT-enheten och Upphandlingsenheten.

I kravställningen på leverantör ska följande beaktas.

- Ska innefatta stöd och support gällande fel och incidenter, reglera hur kontroll av avtalets uppfyllande ska ske.
- Ska reglera ansvar och upprätthållande av implementation och upprätthållandet av IT-säkerhetsfunktioner samt ansvar för testning och verifiering av dessa.
- Ska reglera ansvar för sådana brister som eventuellt upptäcks under drift.
- Bör innefatta att säkerhetstestning av systemet och ingående komponenter ska göras innan leverans av tredje part.
- Ska innefatta att leverantören åtgärdar eventuella säkerhetsbrister som identifierats i samband med acceptanstest och eller leveranskontroll.
- Bör innefatta att källkodsdeposition, där minst ett exemplar av källkoden lämnas i förvar hos tredje part. Detta för att säkerställa tillgänglighet till källkod samt underhåll och utveckling i händelse av oväntade förändringar hos leverantör eller dess underleverantörer.

Ytterligare krav för driftleverantör:

- Fördjupade krav på leverantörens interna IT-miljö
- Kontinuitetshantering
- Rätt till tredjepartsrevision
- Sekretessavtal
- Rätt till incidentrapporter från leverantören

5.8 IT-säkerhetsincidenthantering

IT-säkerhetsincidentrutinen som är en del av incidentprocessen ska användas för att säkerställa ett konsekvent och effektivt tillvägagångssätt för hantering av IT-säkerhetsincidenter inklusive kommunikation. IT-säkerhetsincidentledare leder hanteringen av IT-säkerhetsincidenter i samverkan med relevanta roller i objektorganisationen. Allvarliga IT-säkerhetsincidenter ska dokumenteras i Allvarlig incidentrapport. Det ska finnas en aktuell och tillgänglig IT-säkerhetsincidentrutin samt mall för rapport.

Erfarenheter från inträffade IT-säkerhetsincidenter, t.ex. genom rapporter och statistik, ska ligga till grund för framtida beslut för att förbättra skyddet, t.ex. att investera i nya säkerhetslösningar.

IT-säkerhetsincidenter där brott eller misstanke om brott föreligger ska alltid polisanmälas och insamling av bevis m.m. ska inte göras utan samråd med polisen.

5.9 Granskning och kontroll

För att upprätthålla tillräcklig säkerhetsnivå i objekten Teknisk plattform och IT-arbetsplats ska granskning av IT-säkerhet för IT-komponenterna ske regelbundet för att kontrollera att inga uppenbara sårbarheter exponeras.

Sårbarheter och brister som upptäcks vid granskningar ska införas i objektplaner för åtgärd. Akuta sårbarheter och brister ska åtgärdas omedelbart. Rapportering av större sårbarheter och brister ska ske.