2013-10-30 Ks 1064/2013

Riktlinjer för informationssäkerhet

Örebro kommun

PROGRAM
POLICY
RIKTLINJE
HANDLINGSPLAN

ÖREBRO

Innehållsförteckning

Beslutad av Kommundirektören

1. Inledning

Dessa riktlinjer gäller för alla verksamheter i Örebro kommun. Kommunens bolag beslutar själva om riktlinjer och säkerhetsnivåer inom egen verksamhet.

Eventuella önskemål om undantag gällande Riktlinjer för informationssäkerhet skall ställas till kommunens Informationssäkerhetsråd vilka har till ansvar att bereda önskemålet innan beslut. En riskanalys skall ingå i beredningen av ärendet. Beslut om godkännande av undantag skall fattas av kommunens informationssäkerhetsansvarige i samråd med berörda.

Undantag från Riktlinjer för informationssäkerhet får aldrig vara permanenta utan skall ha en giltighetstid på som längst 2 år. Om behov av undantag kvarstår skall ärendet beredas på nytt och nytt beslut fattas om eventuellt godkännande.

2. Riktlinjer för roller och ansvar

2.1 Basprincip

Ansvaret för säkerheten följer verksamhetsansvaret. Detta innebär att den som är ansvarig för en viss verksamhet också är ansvarig för säkerheten inom respektive verksamhetsområde.

Alla medarbetare inom verksamheten ska känna till att de har ett ansvar för verksamhetens informationssäkerhet. Varje anställd ska i eget arbete följa uppställda regler och givna anvisningar. Varje anställd har även skyldighet att rapportera funktionsstörningar och fel i system, utrustningar och data. Om någon enskild befattningshavare ändå bryter mot gällande styrdokument bär vederbörande själv ansvaret för sitt handlande.

Verksamhetsansvarig, oavsett nivå, ska vid behov utfärda verksamhetsspecifika säkerhetsinstruktioner samt förvissa sig om att de anställda i organisationen har tillräckliga kunskaper för att kunna fullgöra sina arbetsuppgifter. Det åligger varje verksamhetsansvarig att ge sina medarbetare den information och utbildning som krävs för att uppnå en god informationssäkerhet och för att skapa ett säkerhetsansvar hos medarbetarna.

Säkerhetsansvaret i sig kan inte delegeras, däremot kan ansvaret att genomföra vissa arbetsuppgifter fördelas.

2.2 Ansvar på kommunnivå

2.2.1 Kommunstyrelsen

Kommunstyrelsen har det yttersta ansvaret för kommunens informationssäkerhet. Kommunstyrelsen fastställer de centrala säkerhetskrav som ska gälla för verksamheten genom att fastställa kommunövergripande inriktningsdokument.

Kommunstyrelsen utser, i egenskap av personuppgiftsansvarig, personuppgiftsombud för kommunstyrelsens verksamhetsområde. Den personuppgiftsansvarige har alltid det yttersta ansvaret för all behandling av personuppgifter inom sitt verksamhetsområde även om den personuppgiftsansvarige har utsett ett personuppgiftsombud. Om behandlingen sker i strid med personuppgiftslagen eller annan speciallag kan den personuppgiftsansvarige ställas till ansvar, oavsett om han haft uppsåt att handla i strid med lagen eller varit oaktsam.

2.2.2 Kommundirektören

Kommundirektören har ansvar för att informationssäkerhetsarbetet bedrivs i linje med de av kommunstyrelsen fastställda inriktningsdokumenten. Kommundirektören fastställer, på delegation av kommunstyrelsen, kommunövergripande riktlinjer och instruktioner.

2.2.3 Kommunens säkerhetsorganisation

Informationssäkerhetsarbetet i kommunen samordnas av Informationssäkerhetsansvarige på Kommunledningskontorets IT-strategiavdelning. I samordningsuppgiften ingår att samordna, kontrollera och utvärdera informationssäkerhetsarbetet. Informationssäkerhetsansvarige ansvarar för utarbetande av förslag till centrala policydokument, riktlinjer och instruktioner för informationssäkerhet, och utgör ett stöd till verksamheterna.

Vidare ansvarar enheten för beredning samt registrering av ärenden som gäller undantag från kommunens Riktlinjer för informationssäkerhet.

2.2.4 Kommunens revisorer

Kommunens revisorer utför kontroll av informationssäkerheten inom ramen för ordinarie bolags- och förvaltningsrevisioner.

2.3 Ansvar inom varje verksamhet

Varje nämnd är ansvarig för informationssäkerheten inom eget verksamhetsområde. Nämnd kan vid behov besluta om riktlinjer och instruktioner som kompletterar de centralt fastställda. Respektive programnämnd har dessutom ett samordningsansvar för informationssäkerheten inom respektive programområde.

Varje nämnd utser, i egenskap av personuppgiftsansvarig, personuppgiftsombud för den egna verksamheten. Den personuppgiftsansvarige har alltid det yttersta ansvaret för all behandling av personuppgifter, inom eget verksamhetsområde, även om den personuppgiftsansvarige har utsett ett personuppgiftsombud. Om behandlingen sker i strid med personuppgiftslagen eller annan speciallag kan den personuppgiftsansvarige ställas till ansvar, oavsett om han haft uppsåt att handla i strid med lagen eller varit oaktsam.

2.4 Ansvar för säkerheten i verksamhetssystem

2.4.1 Systemägare

Systemägaren är ansvarig för säkerheten för sitt system och ska därvid se till att systemet följer gällande informationssäkerhetspolicy, regler och riktlinjer. Vidare ska systemägaren säkerställa att nödvändiga säkerhetsanalyser och utbildning genomförs för att en godtagbar säkerhetsnivå ska kunna upprätthållas. En del av detta ansvar är att definiera systemets informationssäkerhetskrav.

Systemägaren ska innan nya eller modifierade system får tas i drift förvissa sig om att tillräckliga skyddsåtgärder är vidtagna. Produktionssättning av ett verksamhetssystem ska alltid föregås av ett beslut av systemägaren. Systemägaren ansvarar även för att teckna avtal med personuppgiftsbiträde på delegation av den personuppgiftsansvarige.

I den mån det inte finns en tydlig systemägare följer detta ansvar verksamhetsansvaret.

2.4.2 Informationsägare

För information som endast behandlas i ett (1) system anses systemägaren även vara ägare av informationen. I fallet att en informationsmängd lagras och behandlas i fler än ett (1) system bör en ägare av information utses.

Informationsägaren ansvarar för att informationen sekretessklassas samt fattar beslut om behörigheter till informationen. Även kravställningar och uppföljning av informationssäkerhet i system och applikationer som lagrar och behandlar informationen ingår i detta ansvar.

Om inget annat är uttalat är informationsägaren ansvarig för kvaliteten på informationen.

2.4.3 Systemansvarig

På uppdrag av systemägaren ansvarar den systemansvarige för att systemets krav på informationssäkerhet uppfylls. Systemansvarig ansvarar vidare för att användarna ges nödvändig information och utbildning om systemets säkerhetskrav och skyddsåtgärder.

2.4.4 Drift och förvaltningsorganisation

Drift och förvaltningsorganisationen ansvarar för utförandet av förvaltning och drift av de kommungemensamma IT-systemen. Drift och förvaltningsorganisationen ska tillsammans med de systemansvariga tillse att systemets IT-säkerhet stämmer överens med systemägarens anvisningar så att nödvändig säkerhetsnivå upprätthålls. Man ska också som ansvarig för det interna IT-nätverket ansvara för att detta och informationssystemets tekniska delar fungera och har tillräcklig säkerhet.

2.5 Ny- och vidareutveckling samt avveckling

2.5.1 Projektägaren

Verksamheten äger projektet via en utsedd projektägare. Det åligger projektägaren att säkerställa att säkerhetsfrågorna beaktas.

2.5.2 Projektets styrgrupp

Styrgruppen är ansvarig för att säkerhetsfrågorna beaktas och ska tillsammans med projektägaren fastställa säkerhetsnivån för det system som utvecklas. Under projektets gång ska styrgruppen följa upp hanteringen av de säkerhetsrelaterade frågorna.

2.5.3 Projektledaren

Projektledaren ansvarar för att fastslagen säkerhetsnivå beaktas i projektarbetet.

2.6 Ansvar för leverantör av datatjänster

Leverantör av datatjänster ansvarar enligt upprättade avtal för att levererade produkter och tjänster uppfyller de enligt avtalet specificerade säkerhetskraven. Det

åvilar alltid den som tecknar avtalet att säkerhetskrav enligt Riktlinjer för driftsäkerhet (0) specificeras.

3. Riktlinjer för informationsklassning

All information är känslig och kritisk i varierande grad. För att kunna bedöma om en viss informationsmängd har behov av ett utökat skydd eller särbehandling måste informationen bedömas ur känslighetssynpunkt. Denna process kallas informationsklassning.

3.1 Ansvar

Verksamhetsansvariga på samtliga nivåer i Örebro kommun är ansvariga för att all information som hanteras inom eget verksamhetsområdet hanteras på ett korrekt sätt och ges ett adekvat skydd. Detta gäller oavsett om informationen hanteras elektroniskt eller manuellt. Med detta ansvar följer även ett ansvar för att bedöma informationens skyddsbehov, dvs. klassa informationen.

Information som behandlas av fler än en verksamhet bör ha en (1) utsedd ägare som ansvarar för klassning, hantering och skydd av informationen.

3.2 Arbetsprocess

Klassning skall ske av både information och system. Information skall klassas i sekretessklasser med avseende på krav på sekretess och riktighet hos informationen. System och applikationer skall klassas i tillgänglighetsklasser med avseende på krav på tillgänglighet.

Det skall finnas förutbestämda sekretessklasser och tillgänglighetsklasser samt tillhörande definitioner för respektive klass. Definitionerna skall vara utformade på ett sådant sätt att de tjänar som ett gott stöd i samband med arbetet med informationsklassning.

Revision av informationsklassningen för respektive informationstillgång bör ske minst vartannat år.

3.2.1 Sekretessklassning

Till respektive sekretessklass skall det finnas hanteringsregler som beskriver hur informationen skall hanteras i olika situationer.

All information som hanteras bör klassas, även information som inte lagras och hanteras elektroniskt. I samband med utveckling av nya system skall det säkerställas att den information som är tänkt att behandlas av systemet är klassat.

3.2.2 Tillgänglighetsklassning

Till respektive tillgänglighetsklass skall krav på teknisk arkitektur beskrivas samt eventuella krav på robust infrastruktur som nätverk och försörjningssystem i form av elkraft och kyla.

I samband med utveckling av nya system skall det säkerställas att systemen klassas ur en tillgänglighetsaspekt.

Se även Riktlinjer gällande säkerhetsaspekter vid systemutveckling (0)

3.2.3 Verksamhetsanalys

Denna analys ska ge svar på vilka krav verksamheten ställer på hanteringen av information. Exempel på krav kan vara åtkomst till information vid vissa tidpunkter, att informationen är aktuell och riktig, att information under inga omständigheter får förändras, att det ska vara möjligt att återskapa viss information och att det ska vara möjligt att spåra vem som utfört en viss behandling. Vid verksamhetsanalysen är det viktigt att även ta med i bedömningen att andra delar av organisationen, andra organisationer men även privatpersoner kan påverkas om informationen hanteras felaktigt.

3.2.4 Rättslig analys

För att klarlägga i vilken omfattningen informationen omfattas av särskild eller allmän lagstiftning ska en rättslig analys genomföras. Exempel på rättsliga krav kan vara särskilda gallringsregler, att det föreligger sekretess, att informationen enbart får hanteras i enlighet med fastställda informationen, krav på att information inte får läsas av obehöriga, lagringskrav etc.

4. Riktlinjer för användning av utrustning

4.1 Kommunens utrustning

Samtliga informationssystem och all IT-utrustning som används för behandling och lagring av kommunens informationstillgångar skall vara uppsatta för att stödja och möjliggöra kommunens verksamhet på ett säkert sätt. IT-utrustning som ansluts till Öman- och Pumannäten får endast innehålla program och information som är godkända av kommunen. Kommunen har rätt att granska och ta bort all information som lagras på någon av kommunens IT-utrustning.

Utrustningen är först och främst ett arbetsredskap men visst privat bruk är tillåtet under förutsättning att denna användning inte bryter mot kommunens informationssäkerhetsregler samt ej heller stör eller står i strid med kommunens verksamhet.

Även om viss privat användning av IT-utrustning är tillåtet så betraktas all information som lagras i något av kommunens informationssystem eller IT-utrustning som kommunens egendom.

Internet skall användas av samtliga medarbetare för informationsinsamling i tjänsten och då med sunt förnuft och gott omdöme samt på ett sätt som inte strider mot kommunens etiska regler.

Användning av e-post skall i första hand gälla verksamhetsrelaterad trafik. Privat trafik får förekomma i en begränsad omfattning. Det är inte tillåtet att automatiskt vidarebefordra e-post till externa e-post adresser. Varje medarbetare är skyldig att ansvara för att säkerhet och sekretess ligger i paritet med det material som skickas.

Användning av Internet är endast tillåtet från arbetsstationer. Det är inte tillåtet att använda Internet från servrar eller annan IT-utrustning annat än i de fall som det finns en teknisk tjänst som är installerad på utrustningen som kräver Internetåtkomst.

4.2 Privat utrustning

Privat utrustning får endast kopplas in på kommunens gästnät. Endast kontrollerad och av kommunen godkänd utrustning får kopplas in på kommunens administrativa nät.

Tjänster som görs tillgängliga över internet, exempelvis webbpost, får användas från privat utrustning. Det är däremot inte tillåtet att ansluta via kommunens VPN anslutning från en privat dator.

5. Riktlinjer för personal och säkerhet

Personal med arbetsuppgifter inom IT-området har överlag behov av höga behörigheter till informationssystem och tillämpningar. Med denna typ av behörighet följer ofta indirekt tillgång till stora mängder information. Denna indirekta tillgång till information kan innebära att personal med arbetsuppgifter inom IT-området har möjlighet att missbruka sin behörighet.

5.1 Anställning av personal

I de fall en befattning, vid rekrytering eller befordran, medför att en anställd får tillgång till information och informationsbehandlingsresurser med hög behörighet och särskilt om dessa hanterar känslig information, ska personen alltid lämplighetsprövas.

Motsvarande kontroll ska även genomföras av entreprenörer och tillfälligt engagerad personal, ex från ett personaluthyrnings- eller konsultföretag. Ansvarsförhållanden ska regleras i ett avtal.

Se även Riktlinjer för tredjepartsåtkomst (0).

5.2 Registerkontroll

För vissa särskilt utsatta befattningar som har betydelse för rikets säkerhet, och således omfattas av Säkerhetsskyddslagen (1996:627), ska det i anställningsförfarandet genomföras en registerkontroll. Registerkontrollen ska genomföras innan en person genom anställning eller på annat sätt deltar i verksamhet som har betydelse för rikets säkerhet. De befattningar som är aktuella framgår av Örebro kommuns säkerhetsskyddsplan.

Registerkontrollen administreras av Kommunledningskontoret Säkerhet.

5.3 Sekretessförbindelse

Innan någon tilldelas behörighet till ett IT-system eller annan information, som innehåller uppgifter som är belagda med sekretess, ska alltid prövning av den enskilde ske och en tystnads- och sekretessförbindelse upprättas. Prövningen omfattar en allmän bedömning grundad på personlig kännedom och/eller inhämtade referenser. Upprättandet av en tystnads och sekretessförbindelse ska alltid föregås av utbildning.

Entreprenörer och tillfälligt engagerad personal som inte redan har tystnads- och sekretessförbindelse inskriven i ett existerande avtal ska innan de får tillgång till kommunens informationsbehandlingsresurser upprätta en tystnads- och sekretessförbindelse.

Sekretessavtal bör granskas vid förändringar i anställningsförhållanden eller avtal, särskilt när en anställd är på väg att lämna organisationen, eller när ett avtal löper mot sitt slut. Observera att tystnadsplikten även gäller då anställningen eller entreprenörens avtal upphör.

5.4 Utbildning

Alla användare av kommunens IT-system bör ges en grundläggande informationssäkerhetsutbildning. Utbildningen ska bla. innehålla:

- Relevanta delar av Örebro kommuns informationssäkerhetspolicy med tillhörande riktlinjer.
- Aktuell lagstiftning och säkerhetsföreskrifter.
- Säkerhetsåtgärder som används inom organisationen (informationsklassning, behörighetskontrollsystem, lösenordshantering, skydd mot virus, tillträdeskontroll, skydd av lokaler/utrustning/personal, incidenthantering).

Förutom en grundläggande utbildning ska relevant utbildning ske inom områden som är relaterade till en viss befattning.

Utbildning av samtliga användare skall ske regelbundet och utbildningens innehåll skall hållas aktuell och relevant i förhållande till förändringar av regelverk, lagar, etc.

5.5 Nyckelpersonal

Beroende av nyckelpersonal innebär att verksamheten är mycket sårbar om nyckelpersonal tillfälligt eller permanent uteblir från sin tjänst. Beroendet av nyckelpersonal innebär också att en person ensam kan handlägga ett ärende från början till slut och därigenom, avsiktligt eller oavsiktligt, manipulera eller felaktigt hantera ett ärende.

Respektive verksamhetsansvarig ska aktivt verka för att undvika nyckelpersonsberoende inom den egna verksamheten. I den mån det vid analyser framkommer att organisationen är beroende av nyckelpersonal ska nyckelpersonberoendet åtgärdas ex genom nyanställning eller utbildning av ersättare. Det är viktigt att ersättare ges möjlighet att praktiskt tillämpa sina kunskaper. Nyckelpersonalsberoende kan också minskas genom att använda vedertagen standard och standardprodukter.

5.6 Upphörande eller ändring av anställning

Vid upphörande eller förändring av en anställning skall det säkerställas att eventuella tillgångar som tillhör kommunen skall återlämnas och behörigheter till samtliga system och information tas bort alternativt ändras i enlighet med de behov som förändringen av anställningen medför.

5.6.1 Ansvar vid upphörande av anställning

Ansvaret för att säkerställa informationssäkerheten i samband med upphörande eller ändring av en anställning skall vara klart definierat.

5.6.2 Återlämnande av tillgångar

I samband med upphörande av en anställning skall de tillgångar som den anställde innehar, vilka tillhör Örebro kommun, återlämnas.

5.6.3 Indragning av åtkomsträttigheter

Åtkomsträttigheter till information och system skall snarast avslutas i samband med att en anställning upphör.

Om en anställd avslutar eller ändrar sin anställning och där denne har kännedom om lösenord till gemensamma (opersonliga) användarkonton skall lösenordet för dessa användarkonton ändras snarast.

6. Riktlinjer för fysisk säkerhet

Fysisk säkerhet syftar till att skydda organisationens lokaler, utrustning och informationskapital. Brister i fysisk säkerhet kan medföra att de logiska säkerhetsskydden sätts ur spel. Fysisk säkerhet handlar inte enbart om skydd mot kriminella handlingar, exempelvis inbrott och stöld. Brand, översvämning, oväder eller kraftig åska samt olyckor och katastrofer som orsakas av fel i tekniska system eller mänskliga misstag utgör ett minst lika stort hot mot organisationens informationstillgångar. Det är viktigt att påpeka att skyddsåtgärderna för pappersbunden information och digitalt lagrad information skiljer sig åt avsevärt.

Skyddet bör ha funktioner för att förebygga, upptäcka och återställa. Skyddets nivå ska stå i proportion till förekommande risker. Vid utformning av fysiskt skydd ska åtgärderna och utrustningen som används i möjligaste mån följa vedertagna normer och/eller svensk standard. Dimensioneringen av det fysiska skyddet måste alltid ske från fall till fall och påverkas bl. a av byggnadens konstruktion, läge och vilken typ av utrustning och information som hanteras.

6.1 Skalskydd

Lokaler och dess utrustning ska alltid skyddas med ett skalskydd i skyddsklass 1, 2 eller 3. Eftersom ett hundraprocentigt skalskydd – skalskydd som med säkerhet motstår ett kompetent och målinriktat angrepp – är svårt att skapa, är det oftast nödvändigt att komplettera skalskyddet med andra skyddsfunktioner.

6.2 Tillträdesskydd

Utformning av tillträdesskyddet måste alltid utgå från vilken information som hanteras, hur stöldbegärlig utrustningen är och hur många personer som rör sig i lokalerna.

Utrymmen som har särskilda säkerhetskrav är till exempel rum som används för servrar, modem och annan kommunikationsutrustning, kontorsutrymmen där känslig information bearbetas samt arkiv. Denna typ av utrymmen ska utformas så att endast behöriga personer ges tillgång till utrustning och information.

Extern och egen personal, som inte har behörighet, bör övervakas kontinuerligt då de ska utföra arbete i ett säkrat utrymme.

Det ska finnas skriftliga regler för vem som har tillträde till utrustningen och informationen. Nyckel-, kort- och kodinnehav ska vara förtecknade.

Speciellt känslig utrustning och utrustning som behandlar känslig eller kritisk information bör placeras så att onödigt tillträde minimeras och så att utformningen av punktskydd för utrustningen underlättas.

6.3 Stöldskydd

Ett adekvat skydd mot stöld av datorutrustning och information ska alltid finnas. Skyddet ska anpassas till verksamhetens och informationens skyddsbehov och till de yttre förutsättningarna dvs. lokaler, tillträdesskydd och liknande. Ett fullgott

stöldskydd uppnås normalt genom en kombination av rutiner för hantering av besökare till verksamheten, uppmärksam personal, märkning och fastlåsning av utrustning och/eller inbrottsskydd.

Utrustning ska förtecknas i en inventarieförteckning – gärna kopplad till stöldskyddsmärkningen.

6.4 Avgränsade utrymmen för godsmottagning och lastning

Utrymme för godsmottagning och lastning bör organiseras så att de dels beaktar verksamhetens effektivitetskrav, dels begränsar onödigt tillträde till känsliga områden. Inkommande gods ska registreras och godkännas av egen personal vid leveranstillfället och eventuella avvikelser från förväntad leverans ska kvitteras av leverantören.

6.5 Driftmiljö

För att förhindra förlust, skada eller påverkan på tillgångar och avbrott i verksamheten ska IT-utrustning inte bara skyddas mot stöld och sabotage utan även mot hot och risker i omgivningen, ex störningar i elförsörjning, klimatrelaterade hot och brand. Beroende på driftmiljö måste åtgärderna vara mer eller mindre omfattande. Skyddet av den enskilda driftmiljön måste dimensioneras med hänsyn till de konsekvenser som skulle kunna uppstå.

6.5.1 Elförsörjning

De vanligaste orsakerna till störningar i elförsörjningen är avgrävda kraftkablar, åska och kraftvariationer som kan bero på bland annat fläktregulatorer och hissmotorer. Ett genomtänkt skyddssystem mot störningar i elförsörjningen är A och O för ett effektivt tillgänglighetsskydd. För särskilt avbrottskänsliga eller kritiska IT-system bör skyddsåtgärder som garanterar kontinuerlig strömförsörjning övervägas, ex UPS och reservkraft.

6.5.2 Kyla

Åtgärder ska vidtas för att temperaturen i utrymme där utrustning förvaras, hålls inom de gränsvärden som specificerats för aktuell utrustning. För särskilt avbrottskänsliga eller kritiska IT-system bör kylanläggningens funktion kunna garanteras även vid störningar i elförsörjningen.

6.5.3 Vätskeskydd

För att minimera risk för vattenskador på utrustning bör det inte finnas vattenledningsrör som kan orsaka översvämning i eller i direkt närhet av driftmiljön. I den mån golvbrunn finns ska åtgärder vidtas för att undvika att vatten kan tränga upp bakvägen. Det är även lämpligt att förse driftmiljö med ett vätskelarm.

6.6 Brandskydd

Brand utgör alltid en risk som är viktigt att ha rätt skyddsåtgärder mot oavsett om informationen är pappersbunden eller digital. Verksamhetens lokaler ska övervakas på ett sådant sätt att brand kan upptäckas på ett mycket tidigt stadium.

Servrar och kommunikationsutrustning som är avsedda för flera användare ska placeras på ett ur brandsynpunkt betryggande sätt. Utrymmet ska förses med ett lämpligt branddetekteringssystem. Släckutrustning ska väljas så att inte onödig skada uppstår vid släckning av brand. I de fall till- och frånluft ska finnas i datorrummet ska dessa ovillkorligen förses med brandspjäll där de går igenom brandzonen (väggen). Spjällen ska styras av branddetekteringssystemet i rummet. Utrymmet bör vara utformat så att utrustningen inte utsätts för vätskeläckage, korrosiva brand och släckgaser, damm etc.

Ofta är det inte den direkta branden i driftmiljön som är det största hotet mot verksamheten. Även då branden är belägen i en annan del av byggnaden, är risken överhängande att brandgaser och/eller vattenånga tränger in i datorrummet och att temperaturen i datahallen stiger över 70 °C vilket kan leda till att utrustningen riskerar att gå förlorad. Även om backuputrustning och media placeras på avstånd från datorhallen, men i samma huskropp finns en risk att båda platserna slås ut vid ett tillbud.

Datamedia som innehåller för verksamheten kritisk information och systeminformation ska förvaras brandsäkert i för datamedia brandklassat datamedieskåp. Observera att magnet- och optiskmedia riskerar att förstöras redan vid 55°C.

Hantering av pappersbaserad information i den dagliga verksamheten bör ske genom utnyttjande av brandsäkra närarkiv eller brandsäkra dokumentskåp. Det utökade dokumentskyddet som stängda dörrar ger vid brand måste framhållas.

6.7 Kablageskydd

Starkströmsledningar samt data- och telekablar bör skyddas mot sabotage och avlyssning samt elektromagnetisk störning. Kablage som kanaliseras genom obevakade utrymmen bör alltid skyddas mot insyn.

6.8 Säkerhet för utrustning utanför egna lokaler

Risker i samband med användning av utrustning utanför de egna lokalerna måste analyseras särskilt. Detta gäller för informationsbärare i vid mening och omfattar bland annat datorer för distansarbete, bärbara- och handdatorer och pappershandlingar. Vid utformning av skyddsåtgärder måste man beakta att säkerhetsrisker kan variera avsevärt mellan olika platser och vid olika tidpunkter.

Det måste särskilt påpekas att bärbara datorer aldrig får lämnas obevakade i exempelvis en bil eller ett obevakat eller olåst konferensrum under fikarasten!

6.9 Underhåll av utrustning

Förutsättningarna för en störningsfri driftsmiljö är att följa leverantörens rekommenderade underhållsplan för utrustningen.

6.10 Driftlarm

För att tidigt få indikationer på att den fysiska driftmiljön försämrats bör det finnas olika typer av driftlarm. Exempel på larm är förekomsten av vatten på golvet, hög

temperatur, hög eller låg luftfuktighet, larm från UPS, larm från de tekniska funktionerna i kylmaskinen, tidigt larm från branddetekteringen etc. Om gränsvärden överskrids ska larm skickas till drift- och/eller servicejour.

7. Riktlinjer för styrning av kommunikation

Örebro kommun tillhandahåller olika typer av nätverk innehållandes olika tjänster till kommunens verksamheter.

- ÖMAN – Kommunens administrativa nät [mer beskrivande text för nätets syfte och övergripande säkerhetsregler (på policy nivå)]
- PUMAN – Kommunens ”skolnät” [mer beskrivande text för nätets syfte och övergripande säkerhetsregler (på policy nivå)]
- Gästnätet – Gästnät med enbart tillgång till Internet [mer beskrivande text för nätets syfte och övergripande säkerhetsregler (på policy nivå)]

7.1 Säkerhet vid datakommunikation – allmänt

Datakommunikationen är en kritisk del av IT-systemen. Målet är att säkerställa skydd av information i nätverk och infrastruktur. För att möta kraven på tillgänglighet, riktighet, sekretess och spårbarhet måste stor uppmärksamhet fästas på riskerna för:

- avbrott och störningar
- obehörig åtkomst till nätverket
- avlyssning av förbindelser

De åtgärder som bör vidtas för att förhindra eller minska dessa risker inkluderar:

- redundans och fysiska skyddsåtgärder
- begränsning av åtkomstmöjligheterna till nätverket
- skydd av överförd information

Nätverk bör vara adekvat administrerade och övervakade för att upprätthålla god säkerhet för system och tillämpningar som nyttjar nätverket vilket även inkluderar information under överföring.

Nätverk skall vara logiskt och i förekommande fall fysiskt uppdelade för att skydda information och obehörig åtkomst till system och applikationer.

Där krav finns på starkt skydd mot obehörig åtkomst till information eller där informationens riktighet förblir intakt skall det finnas metoder för kryptering av kommunikationslänkar eller informationen i sig.

7.2 Kryptering av trafik

Om det är möjligt att få obehörig åtkomst till information som skickas över en kommunikationslänk skall kommunikationslänken vara krypterad alternativt skall informationen som skickas vara krypterad. Kryptering kan även med fördel användas för att garantera informationens riktighet.

Observera att det på marknaden finns många olika varianter på krypteringslösningar. Val av lösning måste alltid utgå från behovet.

7.3 Fasta förbindelser

Fast förbindelser till ÖMAN-nätet ska, om inte särskilda skäl föreligger, ske via svartfiber.

Endast kommunala verksamheter får anslutas till ÖMAN-nätet, eventuella undantag behandlas enligt **Fel! Hittar inte referenskälla.**

Vid åtkomst till ÖMAN-nätet via Internet ska alltid tvåfaktorsautenticering av användarna ske. All trafik ska vara skyddad med stark kryptering.

7.4 Extern anslutning

Vid extern anslutning till ÖMAN- och PUMAN-näten med managerad utrustning skall stark autentisering användas. Med stark autentisering menas att man autentiserar genom något man vet, exempelvis ett lösenord, samt något man har, exempelvid en säkerhetsdosa (jmf bankdosa) eller en engångskod som skickas till användaren på ett säkert sätt.

Vid automatisk eller schemalagd anslutning till ÖMAN-nätet kan autenticering även ske med en metod som bygger på nyckel- och certifikatshantering. I sådana fall bör skalskyddet runt den anslutande maskinen säkerställas. Dessutom ska åtkomst till olika resurser och information som finns på ÖMAN-nätet begränsas till det absolut nödvändigaste.

Vid anslutning till ÖMAN-nätet skall informationen, då den skickas över nätverken, skyddas i enlighet med de regler som följer av informationsklassningen.

Kommunikationsutrustning som inte används under längre tid ska vara avstängd eller bortkopplad från interna nätverk.

7.5 Internetanslutningar

Fysiska anslutningar till Internet från något av Örebro kommuns nätverk ska administreras centralt.

Det är inte tillåtet att ansluta utrustning till ÖMAN-nätet som kan fungera som en nätverksbrygga mellan ÖMAN-nätet och Internet.

Anslutning av publika miljöer ex forskarsalar får inte ske via ÖMAN-nätet.

Servrar som måste vara i direktkontakt med Internet, ex webb- och e-postservrar ska alltid placeras i skydd av brandvägg och separerad från det lokala nätet.

Om inga särskilda skäl föreligger bör datorer på PUMAN-nätet välja privata IP-adresser då dessa inte är direkt åtkomliga över Internet vilket ger ett visst skydd mot externa hot. För att skydda sig mot interna hot är det nödvändigt att införa brandväggsfunktionalitet.

7.6 Nätverkssegmentering

Nätverk och, där behov föreligger, nätverkssegment skall åtskiljas med hjälp av tekniska skydd. Access till och mellan nätverkssegment skall styras och kontrolleras med hjälp av brandväggar.

Trafik till och från följande nätverk och nätverkssegment skall styras och kontrolleras med hjälp av brandväggar:

- ÖMAN
- PUMAN
- Gästnätet
- Nätverkssegmentet för administration av nätverksutrustning

Kommunikation som rör styr- och reglersystem samt passer- och larmsystem bör ske på separata logiska nätverkssegment. Synnerligen viktiga system ska skyddas med väl kontrollerad åtkomst.

7.7 Brandväggar

Hårdvarubaserade brandväggslösningar är att föredra. I den mån mjukvarubaserade brandväggslösningar används får inte brandväggsdatorn användas för andra ändamål. Brandväggsdatorn ska alltid vara placerad på ett sådant sätt så att obehörig fysisk åtkomst förhindras.

Konfigurering av brandväggen ska ske i enlighet med en brandväggspolicy. Av brandväggspolicyn ska framgå vilka nätverkstjänster som ska tillåtas. Vidare ska det av brandväggspolicyn framgå vilka händelser och aktiviteter som ska loggas. Loggresultatet ska följas upp i enlighet med fastställd rutin. Befarade oegentligheter samt identifierade intrångsförsök ska alltid dokumenteras.

Se även riktlinjer för loggning av IT-resurser i Örebro kommun (0).

Brandväggen ska revideras periodiskt. Revisionen syftar till att kontrollera att brandväggen är konfigurerad korrekt och i enlighet med gällande brandväggspolicy och att programvaran är uppdaterad. Vid dessa revideringar bör extern opartisk kompetens utnyttjas.

7.8 Trådlösa nät

All utbyggnad av trådlösa nät ska följa kommunens standard.

För all användning av WLAN som medger åtkomst till kommunens nät ska alltid adekvat säkerhet säkerställas.

7.9 Anslutning av datorutrustning på ÖMAN-nätet

För att undvika driftstörningar i kommunikation och verksamhetssystem ska all utrustning som ansluts till ÖMAN-nätet följa kommunens standard. Utrustning ansluten till ÖMANnätet ska alltid ha ett tillfredsställande fysiskt skydd och får inte lämnas obevakad i publika lokaler, ex receptioner eller lärosalar.

7.10 Skydd av extern diagnos- och konfigurationsport

Fysisk och logisk åtkomst till diagnos- och konfigurationsportar på nätverksutrustning skall styras. Detta ska ske genom att:

- Nätverksutrustning ska ha ett gott skalskydd
- Logisk åtkomst till utrustningen ska ske genom att använda ett personligt användarkonto med tillhörande lösenord.
- Uppkoppling mot utrustningen ska ske via ett dedikerat nätverkssegment (VLAN), med begränsad och kontrollerad åtkomst, och trafiken bör vara krypterad.

8. Riktlinjer för driftsäkerhet

För att säkerställa korrekt och säker drift av utrustning och system ska rutiner för drift av system och nätverk finnas. Behörigheten att ta del av systemsäkerhetsinstruktioner och annan driftdokumentation ska alltid begränsas. Pappersdokument ska då de inte används vara inlåsta i brandklassat säkerhetsskåp. Digitalt lagrade drift- och systemdokumentation bör krypteras.

8.1 Systemsäkerhetsinstruktion

Systemsäkerhetsinstruktionen är ett dokument i vilket krav på tillgänglighet, riktighet, sekretess, och spårbarhet för ett enskilt datasystem anges. Den ska innehålla de samlade krav på säkerhet som ställs på datasystemet. Det är viktigt att systemsäkerhetsinstruktionen formellt fastställs av systemägaren eftersom den ligger till grund för beslut om vilka säkerhetsåtgärder som ska vidtas. Systemsäkerhetsinstruktionen ska ta hänsyn till den övergripande informationssäkerhetspolicyn med tillhörande riktlinjer och instruktioner.

Av systemsäkerhetsinstruktionen bör följande framgå:

- Sekretessklassning på den information som behandlas av systemet
- Tillgänglighetsklassning
- Behörighetstilldelning
- Lösenordshantering
- Loggning
- Säkerhetskopiering
- Hantering av datamedia
- Datakommunikation
- Driftsäkerhet
- Incidenthantering
- Programuppdateringar
- Fysiskt skydd

Bilagor

- Verksamhetsbeskrivning
- Vilka hot och risker som är identifierade

- Konsekvensanalys
- Systemdokumentation
- Driftdokumentation
- Användardokumentation

8.2 Bemanning

Det skall finnas en fastställd bemanningsplan för vilka personer och vilken kompetens som behövs för driften. Även andra kompetenser som är viktiga för driften vid exempelvis ett avbrott ska finnas förtecknade.

Ansvar ska fördelas på olika personer för att minska risken för oavsiktligt eller avsiktligt missbruk. Nyckelpersonsberoenden ska alltid undvikas.

8.3 Tillträdesskydd

Tillträdet till viktiga utrymmen, till exempel central/lokal datahall och operatörsrum, ska vara begränsat. Tillträdet bör minst regleras med hjälp av låssystem med separat nyckelsystem. Beslut om vem som ska ges tillträde ska alltid vara dokumenterat.

Se även Riktlinjer för fysiskt säkerhet (0).

8.4 Driftavtal/överenskommelse

Säkerhetskraven för en organisation som lägger ut hantering och styrning av hela eller delar av sina informationssystem, nätverk och/eller andra datamiljöer ska behandlas i ett avtal.

Ett driftavtal och en överenskommelse bör ur säkerhetssynpunkt omfatta:

- ansvars och rollfördelning
- hur de rättsliga kraven ska uppfyllas, t.ex. rörande hantering av information som berörs av sekretess och hantering av personuppgifter
- vilka åtgärder som ska vidtas för att säkerställa att alla berörda parter, inklusive underleverantörer, är medvetna om sitt säkerhetsansvar
- hur riktighet och sekretess rörande organisationens verksamhetstillgångar kan upprätthållas och testas
- krav på tillgänglighet
- vilka fysiska och logiska åtgärder som kommer att vidtas för att begränsa åtkomsten till organisationens känsliga information till enbart behöriga användare

- åtgärder och ansvar vid avbrott
- revisionsrättigheter
- informationshantering vid avtalets upphörande.

Säkerhetskraven ska framgå av systemsäkerhetsinstruktionen. Se även Riktlinjer för tredjepartsåtkomst (0)

8.5 Standardisering av utrustning

För att öka driftsäkerheten ska enhetlighet vad gäller maskin- och programvara eftersträvas. Det ska finnas standarder för hur maskin- och programvara ska installeras och konfigureras.

8.6 Uppdelning av utvecklings- och driftmiljö

Test- och utvecklingsmiljö ska vara åtskild från driftmiljön eftersom icke testad program- och hårdvara kan orsaka allvarliga driftstörningar, t.ex. oönskad förändring av filer, dataförlust och systemfel. En liknande uppdelning bör också ske mellan utvecklings- och testfunktionerna för att testning ska kunna ske i känd och stabil miljö.

Vid användning av produktionsdata i test- och utvecklingsmiljöer måste hänsyn tas till klassning och de hanteringsregler som gäller för informationen som används.

8.7 Skydd mot datavirus och andra skadliga program

Program och andra informationsbehandlingsresurser är sårbara för datavirus och andra skadliga program. Datavirus används i detta sammanhang som samlingsbegrepp för virus och maskar, trojaner och logiska bomber etc. Åtgärderna mot datavirus och andra skadliga program ska utformas för att vara förebyggande, upptäckande och återställande. Det är särskilt viktigt att försiktighetsåtgärder vidtas för att upptäcka och skydda persondatorer mot datavirus.

8.7.1 Åtgärder mot skadliga program

Kommunen ska skydda programvara, data och datorer, nätverk etc. på följande sätt:

- Alla användare ska känna till vilka åtgärder de kan vidta för att minska risken att drabbas av virus och annan skadlig kod.
- Det ska finnas en fastställd rutin för att sprida virusvarningar i kommunen.
- För att undvika virus på persondatorer samt minska risken att virus sprids då datorn ansluts till nätverket eller då filer flyttas, ska det på alla persondatorer finnas antivirusprogram installerat. Programmet skall aktiveras då datorn startas och kontrollera minne, hårddisk och övriga datamedia som är anslutna till datorn.

- Programuppgradering av virusskyddet ska ske regelbundet och utförs automatiskt vid anslutning av utrustningen till nätverket. Utrustning som ej är ansluten till nätverket ska regelbundet uppdateras manuellt.

- Även fil- och applikationsservrar bör förses med antivirusprogram för att undvika att infekterade filer lagras i nätverket eller sprids vidare.

- För att undvika att virus sprids via e-post ska e-postserver alltid förses med antivirusprogram.

- Försiktighet ska alltid vidtas vid hantering av flyttbara datamedia som exempelvis USB minnen, CD, DVD och mobiltelefoner. I möjligaste mån bör lagring av information på denna typ av utrustning undvikas.

- Flyttbara datamedia ska alltid viruskontrolleras innan de används i kommunens utrustning. Detta bör ske automatisk utan att användaren märker det.

- Det är inte tillåtet för användare att installera egen programvara. Undantag behandlas enligt **Fel! Hittar inte referenskälla.**

- Det ska finnas en fastställd rutin för återställning av programvara, data och datorer om kommunen skulle drabbas av skadliga program.

- Hård- och mjukvara ska uppdateras regelbundet för att undvika att kommunen drabbas av skadlig kod som inte upptäckts av virusskyddet.

8.8 Säkerhetskopiering

Förutom behovet av säkerhetskopia vid rena katastrofsituationer finns behov att i efterhand kunna återskapa informationen per en viss dag eller bearbetning bakåt i tiden. Det kan t ex vara i samband med felsökning eller rekonstruktion vid felaktigheter som framkommit i efterhand. Det kan också finnas lagstiftning som kräver att kopior av informationen ska kunna återskapas.

Säkerhetskopieringen syftar till att all väsentlig information ska kunna rekonstrueras med hjälp av säkerhetskopior och återlagringsrutiner. Undantaget är den information som tillförts systemet efter senaste säkerhetskopiering. Hur stor informationsförlust som kan accepteras definieras för varje system och tillämpning. Systemägaren/verksamhetsansvarig ska tillsammans med kommunens IT avdelning fastställa kraven för säkerhetskopiering av information. Dessa krav ska minst reglera vilken information som skall omfattas av säkerhetskopiering, intervall för säkerhetskopiering, hur många generationer av säkerhetskopior som ska finnas samt hur säkerhetskopior ska förvaras och vilka kontroller som ska genomföras av att säkerhetskopiorna är läsbara.

För att säkerställa att säkerhetskopiering sker bör all säkerhetskopiering automatiseras och ske utan att användarna behöver utföra några särskilda åtgärder.

Även information som lagras på datorer vilka ej är anslutna till nätverket bör säkerhetskopieras. I den mån det ej är möjligt att automatisk säkerhetskopiera bör användaren instrueras om hur han/hon kan säkerhetskopiera informationen.

8.8.1 Beställning av återlagring

Rutin och instruktion för hur beställning av återlagring av information genomförs ska finnas. Rutinen skall förhindra obehörig åtkomst till information.

8.8.2 Hantering av säkerhetskopior

Hantering av säkerhetskopior ska alltid ske i enlighet med verksamhetens krav på tillgänglighet, riktighet, sekretess och spårbarhet. Detta innebär att funktioner för att säkerställa en korrekt hantering även omfattar säkerhetskopior.

8.8.3 Förvaring av säkerhetskopior

Förvaring av säkerhetskopior ska ske i särskilt säkerhetsarkiv. Säkerhetsarkivet ska vara utformat för att ge skydd mot brand, stöld, miljörelaterade hot som fukt mm.

Det bör finnas tillgång till två säkerhetsarkiv, ett för korttidslagring och ett för långtidslagring. Åtminstone långtidslagringsarkivet ska vara geografiskt åtskilt från originalmaterialet. Då arkivet för korttidslagring ej är geografiskt åtskilt från originalmaterialet ska säkerhetskopiorna förvaras i ett för datamedia brandklassat säkerhetsskåp.

Rutinerna för hantering av säkerhetskopiorna ska vara utformade så att oavsett från vilket säkerhetsarkiv säkerhetskopiorna tas ska vid en återlagring, ett acceptabelt och komplett resultat erhållas.

8.8.4 Återlagringstest

För att säkerställa att återlagringen fungerar som avsett ska återlagring från säkerhetskopia regelbundet testas. Eftersom återlagringen påverkas av filstruktur, filsystem, operativsystem, hårdvara, konfiguration mm måste återlagringstest utföras i en miljö som i möjligaste mån är en kopia av driftmiljön.

Hur en återlagring från säkerhetskopia ska genomföras ska vara dokumenterad i mycket detaljerade instruktioner, sannolikt för varje enskilt system. Detaljerade instruktioner bidrar även till att bygga bort nyckelpersonsberoenden.

8.9 Hantering och avveckling av datamedia

Datamedia, som innehåller information som är känslig ur spridningssynpunkt, ska vid transport/förvaring utanför verksamhetens lokaler alltid vara kontinuerligt övervakad eller krypterad.

Se även Riktlinjer för fysiskt säkerhet (0)

Datamedia som innehåller information som är känslig ur spridningssynpunkt får inte skickas i väg på reparation utan att särskilda säkerhetsåtgärder vidtas. Åtgärderna ska garantera att datamedia vid leverans ej kommer på avvägar och att leverantör som ska reparera kan hantera denna typ av information. Leverantören ska skriftligen kunna styrka att hanteringen kan ske på ett korrekt sätt.

Vid avveckling av datamedia ska alltid hänsyn tas till att datamedia kan ha innehållit information som är känslig ur spridningssynpunkt. Om denna typ av information hanterats ska datamediet förstöras eller skrivas över så att informationen ej kan återskapas.

Vid all form av avveckling av datamedia ska alltid den kommungemensamma arkiveringsplanen för bevaring/gallring av allmänna handlingar följas.

9. Riktlinjer för styrning av åtkomst

Åtkomstskyddets funktion ska säkerställa att information endast hanteras av behöriga och ska finnas i alla informationssystem.

Grundläggande principer

- Användare ska endast ges tillgång till den information och de informationsbehandlingsresurser som han/hon har behov av för att kunna fullgöra sina arbetsuppgifter.
- Användaren ska i sitt arbete ej uppleva några begränsningar så länge han/hon håller sig till eget tilldelade arbets-/behörighetsområde.
- Nivån på åtkomstskyddet ska relateras till hur informationen bedömts ur känslighetssynpunkt.
- Alla användarkonton och tillhörande behörigheter ska revideras regelbundet.
- Det ska alltid vara möjligt att härleda en handling till en enskild person eller viss systemresurs.
- För persondatorer som används fristående av en person gäller att användaren ska ha full kontroll över att ingen annan än behöriga utnyttjar persondatorn. Detta kan uppnås antingen genom ett behörighetskontrollsystem, kryptering eller genom ett fullgott fysiskt skydd.

9.1 Behörighetskontrollsystem

Behörighetskontrollen är grunden för åtkomstskyddet. Behörighetskontrollen består av tre delar; identifiering och autenticering, åtkomstkontroll samt uppföljning.

Identifiering ska ske med hjälp av ett användar-ID vilket ska vara unikt för respektive användare. Autenticering, som är processen för att kontrollera en uppgiven identitet, ska normalt ske med hjälp av ett lösenord som är knutet till respektive användar-ID. I vissa fall, till exempel vid önskad åtkomst till känslig information, kan krav ställas på så kallad stark autentisering. Detta innebär att något mer än bara ett lösenord måste uppges, exempelvis någon form av engångskod.

Åtkomstskyddet bygger på att det till respektive användar-ID kopplas en behörighet att använda viss information, t.ex. läsa, skriva, ändra, radera. Åtkomsten till information ska utgå från vad varje användare har behov av för att kunna utföra sitt arbete. I de fall då grupper av användare har samma eller liknande behov av behörigheter bör så kallad roll- eller gruppbaserade behörigheter användas. Sådana roller eller grupper ska alltid dokumenteras.

Uppföljning innebär att allt som har betydelse för säkerheten i systemet loggas. Försök till obehörig åtkomst till andra resurser än de som är tillåtna ska loggas av behörighetskontrollsystem. Hur loggning får ske i Örebro kommun framgår i Riktlinjer för loggning (0).

9.2 Behörighetsadministration

9.2.1 Användarregistrering

Åtkomstskydd förutsätter en väl fungerande användarregistrering. Vid användarregistreringen ska alltid nedanstående formella rutiner användas:

- Verksamhetsansvarig ska skriftligen bevilja registrering av ny användare. Verksamhetsansvarig ska även skriftligen bevilja förändring i behörighet för enskilda användare.
- Varje användare skall tilldelas ett användar-ID som skall vara personligt och unikt.
- Alla användare ska vara registrerade i en förteckning.
- Ej giltiga behörigheter ska kontinuerligt ta bort för att undvika att personer som slutat sin anställning eller bytt arbetsuppgifter finns kvar i datorsystemen.

Rutiner och ansvar för borttagning av användar-IDn och behörigheter i samband med avslutande eller annan förändring av anställning ska finnas.

9.2.2 Särskilda åtkomsträttigheter

Tilldelning och utnyttjande av särskild åtkomsträtt vilket tillåter användare att gå förbi spärrar för system- och tillämpningar ska begränsas. Systemansvarig beslutar om tilldelning av särskild åtkomsträtt. Rutinerna för tilldelning av särskilda rättigheter följer de rutiner som beskrivs under användarregistrering. Tilldelning av dessa rättigheter ska alltid ske individuellt. Användning av grupper är inte tillåten. Särskilda rättigheter bör tilldelas med användning av annan användaridentitet än den som utnyttjas i den normala verksamheten.

9.2.3 Granskning av åtkomsträttigheter

Ett minimikrav är att allmänna åtkomsträttigheter på gruppnivå ska granskas en gång per år medan granskning av särskilda rättigheter ska ske på individnivå en gång per halvår. Vid granskningen ska en bedömning göras om åtkomsträttigheterna ligger på en adekvat nivå. Vid behov korrigeras åtkomsträttigheterna. Alla användare ska meddelas om åtkomsträttigheterna och därmed villkoren för åtkomst förändras. Vid granskning ska även kontrolleras att åtkomsträttigheterna inte erhållits otillbörligt.

9.3 Lösenordshantering

Lösenord är en av de vanligaste metoderna att validera en användares rätt till åtkomst av ett informationssystem. Lösenordsrutinen ska erbjuda en metod som säkerställer lösenord av god kvalitet.

Bra lösenord uppnås genom att:

- Lösenordet är konfidentiell information och ska förvaras skyddat av användaren. Lösenord ska bytas direkt om misstanke finns att det har röjts.
- Lösenordet ska vara konstruerat så att det inte kan förknippas med användaren. Det bör omfatta minst 8 tecken, blandat siffror, bokstäver och specialtecken.
- Det ska finnas metoder för att säkerställa en användares identitet innan denne tilldelas ett nytt temporärt lösenord.
- Tillfälliga lösenord ska vara unika och inte enkla att gissa.
- Tillfälliga lösenord skall endast vara giltiga för en (1) inloggning.
- Tillfälliga lösenord skall tilldelas användare på ett säkert sätt
- Byte av lösenord bör ske med lämpliga intervall, högst 90 dagar.
- Funktion för att styra bort olämpliga lösenord bör finnas.
- Tidigare använda lösenord bör inte gå att återanvända inom 13 månader.
- Lösenord får aldrig skickas/transporteras i klartext över nätverk. Varken tilldelning av lösenord eller vid användning av lösenord för autentisering.
- Lösenord ska lagras krypterat och, om möjligt, skilt från tillämpningssystemen.
- Om felaktigt lösenord används mer än fem gånger ska användaren utestängas ur systemet och händelsen loggas.
- Samtliga datorer bör förses med lösenordsskyddad skärmsläckare. Denna ska ej vara möjlig att inaktivera.

Om känslig information hanteras bör ett starkare skydd eftersträvas. Detta skydd kan byggas utifrån att andra metoder för autenticering används alternativt att mycket högre krav på punkterna ovan tillämpas. Användning av lösenord möjliggör ej heller att man med säkerhet kan knyta en användare till en viss handling.

9.4 Tidsfördröjd utloggning vid inaktivitet

I den mån utrustning som är installerad i externa lokaler eller i lokaler som är allmänt tillgängliga och som hanterar känslig information eller där det föreligger risk för att utrustningen missbrukas, bör funktioner för utloggning efter en definierad tids inaktivitet användas. Vid utloggningen ska skärmen rensas och både tillämpnings- och nätverkssessioner bör avsluta.

9.5 Riktlinjer för tredjepartsåtkomst

Samma nivå på informationssäkerheten krävs oavsett om informationsbehandlingen sker med interna resurser eller av tredjepart. Tredjepart kan medges åtkomst av flera olika skäl. Gemensamt för all tredjeparts åtkomst är att åtkomsten kan orsaka svagheter i fråga om säkerhet. Där verksamheten har ett behov av att tillåta tredjepartsåtkomst bör en riskanalys göras för att identifiera vilka krav som ska ställas på åtkomstskyddet. Därvid bör följande beaktas, typ av åtkomst som är nödvändig, informationens värde till vilken åtkomst ges, de styrmedel och åtgärder som tredjepart tillämpar och de följder som åtkomsten kan ha för säkerheten hos organisationens information. Det är väsentligt att tredjepart har förståelse för vilka säkerhetsåtgärder som krävs för att administrera tredjepartsåtkomst till organisationens informationsbehandlingsresurser.

9.5.1 Definition

Med tredjeparts åtkomst avses externa användare såsom tillfälligt anställda och praktikanter såväl som konsulter. Dessutom omfattas extern leverantör som utför drift- och eller förvaltningsuppdrag åt kommunen.

9.5.2 Principer

Externa användare

- extern användare ska ha kännedom om verksamhetens informationssäkerhetspolicy, regler och riktlinjer samt följa dessa
- extern användare ska endast få tillgång till de informationssystem/data som ansvarig i verksamheten godkänt åtkomst till
- sekretessavtal mellan ansvarig på verksamheten och extern användare ska alltid upprättas om det inte är uppenbart att kontakt med känslig information ej kan förekomma
- konsulters skyldigheter ska alltid regleras i avtal

Extern leverantör

- om en organisation lägger ut hela eller delar av sin drift eller förvaltning överlåts även det operativa ansvaret för informationssäkerheten till serviceföretaget
- nivån för informationssäkerheten ska regleras i avtal med serviceföretaget
- extern driftleverantör ska ha god kunskap om och kommunens informationssäkerhetspolicy, regler och riktlinjer

Ett avtal med en tredje part kan t.ex. innehålla:

- Relevanta delar av kommunens informationssäkerhetspolicy.
- Beskrivning av de delar av verksamheten som berörs och under vilka tider.

- Restriktioner beträffande kopiering och spridande av information.
- Åtgärder för att återlämna/förstöra information som har gjorts tillgänglig under avtalstiden.
- Regler för tystnadsplikt och sekretess.
- Krav på att upprätta och hålla aktuell förteckning över berörda tredjepartspersoner och villkor för att engagera underkonsulter.
- Våra rättigheter till revision.

9.6 Hantering av information utanför arbetsgivarens utrustning

Arbetsgivaren ansvarar för att den information som hanteras ges ett adekvat skydd. I vissa fall kan arbetsgivaren bli ansvarig för skador som de anställda orsakar, genom exempelvis felaktig behandling av personuppgifter. Detta gäller oavsett om den anställde hanterar uppgifterna på arbetsgivarens utrustning eller någon annanstans. Eftersom arbetsgivaren enbart kan ställa krav på och påverka sin egen utrustning får inte information som är känslig ur spridningssynpunkt hanteras utanför arbetsgivarens utrustning. Hantering av information som inte är känslig ur spridningssynpunkt bör begränsas.

9.7 Fysiskt åtkomstskydd

Riktlinjer för utformning av den fysiska miljön framgår av Riktlinjer för fysiskt säkerhet (0).

10. Riktlinjer för loggning av IT-resurser i Örebro kommun

För att upptäcka avvikelser från kommunens informationssäkerhetspolicy ska kommunens IT-resurser övervakas. Dessa riktlinjer beskriver kommunövergripande regler för loggning av kommunens datasystem, datanät och IT-baserade tjänster och syftar till att klargöra vilka regler som gäller för loggningen. Däremot syftar dessa riktlinjer inte till att klargöra exakt hur denna loggning ska gå till. Detta måste avgöras från fall till fall.

10.1 Omfattning

Loggning av kommunens datasystem, datanät och IT-baserade tjänster är enbart tillåten då den är nödvändig för att kunna säkerställa driften och säkerhetsnivåerna och för att kunna utföra felsökning. All annan form av loggning är enbart tillåten då det i lagstiftning finns krav på att loggning av händelser ska ske eller då det föreligger misstanke om brott. Föreligger misstanke om brott kommer Örebro kommun att bistå rättskipande myndighet. Utdrag av loggar beslutas av förvaltningschef eller kommunens säkerhetschef.

Vid all loggning av IT-resurser måste alltid skyddet av den personliga integriteten värderas högt.

10.2 Skydd av den personliga integriteten

Örebro kommun tillåter att vissa av kommunens IT-resurser, ex Internet och e-post, används för privata ändamål i den mån den ordinarie verksamheten inte störs, inte skapar merkostnader för kommunen eller att användningen står i strid med gällande lagstiftning eller andra föreskrifter meddelade av Örebro kommun. Detta innebär att det vid loggning kan framkomma information som är av privat natur. I den mån det ej föreligger misstanke om brott mot gällande lagstiftning eller andra föreskrifter meddelade av Örebro kommun föreligger tystnadsplikt för driftpersonal och annan personal som kommer i kontakt med loggningsresultat.

10.3 Uppföljning av loggning

För all loggning som genomförs ska det finnas rutiner för hur loggningen ska följas upp.

10.4 Åtkomst till loggresultat

En viktig del av loggningen är att ge underlag för kontroll av att användare och systemadministratörer inte överträder sina tjänstemässiga befogenheter, därför ska behörigheten att ta del av säkerhetsloggar begränsas.

Alla loggresultat ska skyddas mot obehörig förändring och borttagning. Skyddet ska omfatta både loggresultat och eventuella funktioner som kan förhindra loggning.

Följande principer bör tillämpas:

- Användare som har behörighet att påverka vitala funktioner (system-, nätverks- eller behörighetsadministration) ska inte ha behörighet att radera loggar eller förändra funktioner som styr loggningen.

- Loggar ska inte kunna förändras, utan endast raderas. Raderingen skall samtidigt ge upphov till en ny loggpost.

- Logganalys bör om möjligt utföras i ett system som är logiskt avskilt från det system som analysen avser.

- Rutiner för loggning och analys av loggdata ska vara dokumenterade. Av dokumentationen ska det framgå under hur lång tid loggresultatet ska sparas.

- Lagring av loggningsresultat bör alltid ske åtskilt från det system som loggas.

10.5 Klocksynkronisering

För att loggtransaktioner ska vara möjliga att spåra mellan olika system och för att säkerställa tillförlitlighet hos loggar är en korrekt inställning av datorklockor viktig. Korrekt inställning av klockan kan krävas för utredningar eller vid en eventuell rättslig prövning.

Där dator- eller kommunikationsenheter kan påverka tidssynkroniseringen, bör den ställas till en överenskommen standard. Eftersom vissa klockor kan dra sig med tiden, bör det finnas en rutin som kontrollerar och rättar varje signifikant avvikelse.

10.6 Skyldighet att vidtaga åtgärder

I den mån det vid loggning, som sker som en del av driften, uppdagas verksamhet som står i strid med gällande lagstiftning eller andra föreskrifter meddelade av Örebro kommun, föreligger skyldighet att rapportera händelsen till verksamhetsansvarig som är skyldig att vidtaga åtgärder. Det är ej tillåtet för driftspersonal att på egen hand vidtaga åtgärder om dessa åtgärder inte är nödvändiga för att driften ska kunna garanteras.

11. Riktlinjer gällande säkerhetsaspekter vid systemutveckling

Det skall finnas en fastställd systemutvecklingsrutin som skall följas vid all systemutveckling. Rutinen skall säkerställa att informationssäkerhet är en integrerad del i utvecklingsarbetet samt i det färdiga systemet.

Informationssäkerhetskraven skall framgå av klassningen av den information som skall behandlas i systemet samt ur tillgänglighetsklassningen av det färdiga systemet.

Med säkerhet i systemutveckling avses även alla de aktiviteter och åtgärder som krävs för att det färdiga systemet ska följa kommunens informationssäkerhetspolicy med tillhörande riktlinjer samt gällande lagstiftning.

Redan under förstudie-/förprojekteringsfasen måste de övergripande kraven på säkerhet specificeras. Kostnaderna för att i efterhand införa IT-säkerhetsåtgärder kan bli mångdubbla jämfört med om man redan under projekteringen av ett system tar hänsyn till dessa frågor.

11.1 Lagstiftning och andra styrande dokument

Innan ett systemutvecklingsprojekt startar ska alltid en analys genomföras av vilka styrande dokument som kommer att påverka utvecklingen. Vid analysen ska alltid kommunens informationssäkerhetspolicy med tillhörande riktlinjer och instruktioner samt gällande lagstiftning följas.

11.1.1 Hot- och riskanalys

För att definiera rätt skyddsnivå ska alltid hot och riskanalyser genomföras i den inledande fasen av ett utvecklingsprojekt liksom vid större förändringar av ett informationssystem. Utifrån analysen och informationsklassningen definieras skyddsnivån. Skyddsnivån ska vara definierad och fastställd innan utveckling av IT-system påbörjas.

En fullständig riskanalys omfattar:

- Identifiering av hot och brister.
- Bedömning av sannolikheten för att ett hot realiseras.
- Bedömning av konsekvenser av ett realiserat hot.
- Riskbedömning, d v s konsekvensen av en händelse multiplicerad med sannolikheten för att den inträffar.

De hot som kan ge de största konsekvenserna har oftast låg sannolikhet varför det är svårt att göra en relevant sannolikhetsbedömning. Den avgörande faktorn är därför ofta vetskapen att en sådan händelse faktiskt kan inträffa. Beslut om skydd mot en sådan händelse baseras på om konsekvenserna anses oacceptabla.

11.2 Granskning ur säkerhetssynpunkt

Under utvecklingsarbetet bör, efter hand som de färdigställs, kravspecifikation, systemspecifikation och det färdiga systemet granskas ur säkerhetssynpunkt.

11.3 Programtest

Alla program, såväl anpassade standardprogram som egenutvecklade program, ska testas för att säkerställa att de specificerade funktionerna fungerar på tillfredsställande sätt innan de får tas i produktion. Testerna ska regleras i en testrutin och dokumenteras.

Dessa krav gäller även för program som ska sättas i drift efter ändring.

11.4 Driftsättning

Det ska finnas skriftliga instruktioner för hur ett system eller dess delar förs över från utvecklings- och testfas till drift, såväl vid första driftsättning som efter systemförändringar. Innan ett system eller större förändringar driftssätts ska systemet alltid driftgodkännas av systemägaren.

Driftgodkännandet innefattar även säkerställande av nya eller befintliga kontinuitetsplaner.

12. Riktlinjer för kontinuitetsplanering

Tillgängligheten till system och applikationer ska styras av krav från verksamheten. Dessa krav bör fångas genom en analys av verksamhetens processer och dess behov av information och systemstöd.

Kontinuitetsplaner ska upprättas för att kunna upprätthålla eller återställa tillgänglighet till information och IT-system till den nivå, och inom den tid, som krävs av verksamheten i händelse av avbrott eller fel i IT-system och applikationer.

Ur verksamhetskraven som ligger till grund för kontinuitetsplanen ska det framgå:

- Hur länge en verksamhetsprocess kan stå helt still utan att någon skada sker
- Hur länge en verksamhetsprocess kan klara sig med alternativa rutiner utan systemstöd
- I vilka lokaler som verksamheten planerar att bedriva sin verksamhet i fallet att de ursprungliga lokalerna inte är tillgängliga

Det åligger verksamheten att ta fram samt dokumentera alternativa rutiner för verksamhetsprocesser där så är möjligt.

12.1 Ramverk

Det skall finnas ett ramverk för kontinuitetsplaner som säkerställer att alla planer är konsekventa.

12.2 Kontinuitetsplan

Det skall finnas en kontinuitetsplan per system

Kontinuitetsplanen skall minst innehålla:

- Villkor för att aktivera kontinuitetsplanen
- Identifiering av ansvar och beslutsvägar i ett kontinuitetsläge
- Driftsrutiner för återstart i ursprunglig utrustning i ursprungliga lokaler
- Driftsrutiner för återstart i reservutrustning
- Driftsrutiner för återstart i utrustning i andra lokaler
- Eventuella beroenden av andra system, IT-utrustning, kommunikationsförbindelser, nyckelpersoner, 3:e parts leverantörer samt andra kritiska resurser
- Hur kontinuitetsplanen ska testas

12.3 Förvaring av avbrotts- och katastrofplaner

Dokumentationen är överlag mycket känslig för spridning och ska enbart delges behöriga. Förvaring av dokumentationen ska ske i inbrottssäkert och brandskyddat säkerhetsskåp.

12.4 Ansvar

12.4.1 Systemägare

Respektive systemägare ansvarar för att ta fram kontinuitetsplan för systemen. För de system som inte har utsedda systemägare ansvarar verksamhetsansvarig för att kontinuitetsplan tas fram.

Systemägaren ansvarar även för att respektive plan revideras och hålls aktuell genom övning, tester samt utbildning av personal. I ansvaret ingår även att utbilda nyanställd personal.

12.4.2 Verksamhetsansvarig

Verksamhetsansvariga ansvarar för kontinuitetsplaner för verksamhetsprocesser tillsammans med kravställningar gällande information och systemstöd. Vidare ansvarar verksamhetsansvarig även för att ta fram samt dokumentera alternativa rutiner för verksamhetsprocesser som skall användas i händelse av avbrott.

12.5 Test, underhåll av kontinuitetsplaner

Kontinuitetsplaner bör testas och uppdateras regelbundet för att säkerställa att de är aktuella och verkningsfulla.

Tester av kontinuitetsplaner bör innehålla:

- Skrivbordstester av olika avbrottsscenarier
- Tekniska tester av återstarter i:

- Ursprunglig hårdvara

- Reservhårdvara

- Återläsning av säkerhetskopior
- Test av leverantörsresurser och tjänster
- Fullskaleövningar vilket inkluderar verksamhetsprocesser samt IT-system och infrastruktur.

13. Riktlinjer för internkontroll av informationssäkerhet

Kontroll av efterlevnad av informationssäkerhetspolicyn med tillhörande riktlinjer är en del av kommunens internkontroll. Kontrollerna syftar till att identifiera områden där det finns brister i efterlevnaden och där förändringar i rutiner eller ökade utbildningsinsatser är nödvändiga.

13.1 Ansvar

Kommunledningskontorets säkerhetsenhet har på uppdrag av kommunstyrelsen det övergripande ansvaret för att internkontroll av informationssäkerhet genomförs. Säkerhetsenheten ska även genomföra viss del av internkontrollarbetet.

Respektive verksamhetsansvarig är skyldig att genomföra internkontroll i enlighet med Säkerhetsenhetens direktiv.

13.2 Kontrollområden

Exempel på kontrollområden är:

13.2.1 Administrativsäkerhet

- Kunskap om och efterlevnad av fastställd informationssäkerhetspolicy med tillhörande riktlinjer på ledningsnivå såväl som på användarnivå.
- Efterlevnad av relevant lagstiftning.

13.2.2 Fysisk säkerhet

- Centrala och lokala driftmiljöer
- Placering av kommunikationsutrustning
- Arbetsplatser och kontor
- Arkivlokaler för pappershandlingar respektive datamedia

13.2.3 Logisk säkerhet

- Säkerhetsfunktioner finns implementerade för att uppnå en adekvat säkerhetsnivå.
- Säkerställa att säkerhetslösningar är korrekt implementerade.

Vad som ska kontrolleras fastställs årligen av kommunstyrelsen i en kontrollplan för Informationssäkerhet. Av kontrollplanen ska även framgå hur internkontrollen ska finansieras.

13.3 Arbetsmetoder

Vid internkontroll av informationssäkerhet används ett flertal olika arbetsmetoder, vilka är både administrativa och tekniska. De administrativa kontrollerna kan genomföras i form av enkäter, intervjuer men även hot- och riskanalyser kan användas.

De tekniska kontrollerna används för att säkerställa att säkerhetslösningar är korrekt implementerade. Dessa kontroller är aktiva till sin karaktär och ska alltid utföras av specialister. Tekniska kontroller kan vara så kallade penetrationstester, användning av särskilda analysprogramvara och loggning. Denna typ av tester ska inte genomföras av de som varit delaktiga vid installation och konfigurering.
Vid tekniska tester av säkerheten är det väsentligt att testerna inte äventyrar systemens säkerhet, varför utförandet av testerna alltid ska övervakas av kommunens egen personal. För kontroll av fysisk säkerhet genomförs besiktningar på plats.

13.4 Styrning av kontroll

För att arbetet inte i onödan ska störa den ordinarie verksamheten bör följande iakttas:

- arbetet ska ske i samråd med verksamhetsansvarig, endast i undantagsfall ska överraskande kontroller genomföras
- överenskommelse om vad som ska granskas ska finnas
- verksamhetsansvarig ska bistå med erforderlig personal
- om det finns risk för störningar i befintliga IT-miljöer ska tekniska kontroller ske i testmiljö eller motsvarande
- arbetet ska dokumenteras
- resultat av arbetet ska sekretessbedömas innan det färdigställts

13.5 Delgivning av resultat

Resultatet av internkontroll ska rapporteras till kommunstyrelsen och till berörda verksamhetsansvariga. Rapporten ska följas av ett förslag till handlingsplan för att rätta till eventuella brister.

14. Riktlinjer för användning av Internet, e-post, fax, och telefoni.

Dessa riktlinjer beskriver kommunövergripande regler för informationshanteringen med hjälp av internet, e-post, fax och telefoni. Riktlinjerna gäller generellt för alla anställda, förtroendevalda och andra nyttjare som har behörighet att använda kommunens administrativa resurser för kommunikation. Riktlinjerna syftar till att skydda kommunen och kommunens varumärken, tredje man, enskilda användare samt säkerställa en god driftsäkerhet.

14.1 Omfattning

Riktlinjerna omfattar användningen av Internet, Intranät, e-post, telefoni och fax. Användningen syftar till att underlätta utförandet av ordinarie arbetsuppgifter/verksamhet. All annan användning är enbart tillåten då den:

- inte stör ordinarie arbetsuppgifter/verksamhet.
- inte innebär merkostnader för kommunen
- inte innebär att användningen bryter mot dessa riktlinjer
- inte står i strid med gällande lagstiftning eller lokala föreskrifter meddelade av Örebro kommun

De regler som gäller i samhället i övrigt gäller också användningen av Internet, Intranät, epost, telefoni och fax. Tryckfrihetsförordningen, brottsbalken, lagen om upphovsrätt samt personuppgiftslagen är exempel på lagar som i kombination med dessa riktlinjer och anställningsavtalet bland annat innebär att:

- det inte är tillåtet att uppmana till brott eller sprida någon annans uppmaning till brott,
- det inte är tillåtet att göra eller sprida uttalanden som diskriminerar eller utpekar någons ras, hudfärg, kön, religion, tillhörighet till etnisk grupp eller sexuell läggning,
- det inte är tillåtet att behandla eller sprida pornografiska bilder, pornografiska bilder på barn eller bilder som skildrar grovt våld, tvång eller råhet. Det är ej heller tillåtet att behandla texter med motsvarande innehåll,
- det inte är tillåtet att köpa eller uppmuntra till köp av sexuella tjänster,
- det inte är tillåtet att göra eller sprida uttalanden som är stötande eller ärekränkande för vare sig levande eller döda,
- det inte är tillåtet att medvetet utnyttja resurser på arbetsplatsen för otillbörligt manipulerande eller sabotage av data i den egna organisationen eller externa organisationer,

- det inte är tillåtet att använda andras bilder, texter, musik, filmer etc. som sina egna, dvs. att man respekterar lagen om upphovsrätt,

- det är inte tillåtet att lägga ut personrelaterad information eller bilder på personer utan personernas skriftliga medgivande,

- det inte är tillåtet att sprida reklam för egen personlig vinning eller andras kommersiella verksamhet,

- det inte är tillåtet att på egen hand installera modem eller annan kommunikationsutrustning och på så sätt skapa alternativa vägar för datakommunikation

Vid användning av kommunens IT-system ska beaktas att e-post och fax ska hanteras som vanlig post vad avser handlingsoffentlighet och sekretess.

14.2 E-post

Vid användning av e-post ska alltid regler för registrering och tillhandahållande av allmänna handlingar följas. Det är mycket viktigt att allmänhetens rätt till insyn enligt offentlighetsprincipen inte försämras när e-post används.

14.3 Allmän handling

En handling är allmän om den är förvarad, inkommen till eller upprättad hos myndigheten. Inte bara pappersdokument är handlingar i Tryckfrihetsförordningens mening. Informationen som sådan utgör handlingen oavsett om den består av bild, ljud eller text. Elektroniska handlingar betraktas som inkomna när handlingen är tillgänglig för myndigheten, således inte när en enskild handläggare öppnar försändelsen.

E-post som skickas till personliga brevlådor är allmän handling om innehållet gäller ärende eller annan fråga som ankommer på myndigheten. E-post som är inkommen men som är avsedd för mottagaren i egenskap av befattning eller funktion som ej berör Örebro kommun är ej allmän handling.

14.4 Tillhandahållande av allmänna handlingar

Allmänheten ska kunna ta del av allmänna handlingar hos en myndighet i samma omfattning som myndigheten själv. Bedömningen av en handlings status är en viktig del i upprätthållandet av en god offentlighetsstruktur. Myndigheten är skyldig, efter sekretessprövning, att skyndsamt och i läsbar form tillhandahålla en allmän handling som finns i personliga-, myndighets- eller funktionsbrevlådor, åt den som begär det.

Handlingar är inte allmänna om de:

- är minnesanteckningar, d.v.s. hör till ett ärende utan att tillföra ärendet sakuppgifter

- utväxlas som arbetsmaterial under ett ärendes beredning (mellanprodukter)

- är myndighetsinterna meddelanden och informationsmeddelanden
- är rent personliga meddelanden i ett meddelandesystem
- tas emot av en person i egenskap av annan ställning, t.ex. partipost till politiker eller post till facklig förtroendeman

14.5 Diarieföring av allmänna handlingar

All e-post som är allmän handling ska omgående vidarebefordras till myndighetens registrator.

14.6 Hantering av sekretesskänslig information

Hantering av information som är känslig ur spridningssynpunkt, är enbart tillåten då det finns särskilda funktioner för att förhindra obehörig åtkomst. Val av teknik och nivå bedöms utifrån hot- och riskanalysens resultat. Om dessa funktioner saknas får inte denna information hanteras i e-postsystemet.

14.7 Gallring av e-post

E-post som är allmän handling får gallras, dvs. raderas, från brevlådan först när e-posten diarieförts. I den mån e-postmeddelandet ej är att anse som allmän handling får det raderas omgående.

Vissa e-postmeddelanden som är allmänna handlingar är undantagna från kravet på registrering. Detta gäller meddelanden som bedöms vara av uppenbart ringa eller tillfällig betydelse för kommunens verksamhet, tex reklamförsändelser. Denna typ av allmänna handlingar behöver inte diarieföras och kan raderas från brevlådan efter en vecka[1].

Diarieförda handlingar inklusive e-postmeddelande bevaras/gallras i enlighet med den kommungemensamma arkiveringsplanen.

14.8 Brevlådor

Följande typer av brevlådor används i Örebro kommun:

- Myndighetsbrevlådor (obligatoriska för respektive nämnd).
- Funktionsbrevlådor (t.ex. för enheter).
- Personliga brevlådor.

---

[1] Beslut i KS 29/2 2000

14.8.1 Myndighets- och funktionsbrevlådor

Varje nämnd ska ha en myndighetsbrevlåda tillgänglig för e-post. Även en kommungemensam brevlåda finns, som kan användas när avsändaren ej känner till kommunens organisation. Som komplement till myndighetsbrevlådan kan enskilda förvaltningar eller enheter använda funktionsbrevlådor.

Respektive nämnd eller enhet som använder myndighets- och funktionsbrevlådor är skyldig att utse en ansvarig. Den ansvarige ska bevaka att posten i myndighetsbrevlådan öppnas och vara kunnig i de regler och rutiner som gäller för hantering av allmänna handlingar.

14.8.2 Personlig brevlåda

Med personlig brevlåda avses ett e-postkonto som är knutet till en enskild person. Innehavaren av e-postkonto ansvarar personligen för användandet av e-postkontot. Vid användandet av den personliga brevlådan ska alltid regler för registrering och tillhandahållande av allmänna handlingar följas.

14.8.3 Hantering av personliga brevlådor

För att undvika att inkommen e-post kan förbli oöppnad under en längre tid är den som ansvarar för en personlig e-postbrevlåda skyldig att löpande bevaka sin e-postbrevlåda. Vid längre frånvaro måste hanteringen av e-post säkerställas genom en verksamhetsspecifik rutin.

Då ett e-postkonto upphör exempelvis på grund av att innehavaren slutar eller byter namn ska funktioner finnas för att under rimlig tid meddela avsändaren anledningen till varför meddelandet inte kunde levereras.

14.9 Viktigt att tänka på vid användning av Örebro kommuns e-postsystem

- E-postkontot är personligt. Användarnamn och lösenord får ej överlåtas eller användas av annan person. Kontoinnehavaren är alltid ansvarig för den e-post som skickas från kontot.
- Använd lösenord av god kvalité och byt det regelbundet.
- Det är under inga omständigheter tillåtet att uppträda under annat eller annans namn då e-postsystemet används.
- Alla e-postanvändare ska hålla sig informerade om riskerna med datavirus. Hantera externa dokument och filer med försiktighet och använd de hjälpmedel som finns för att skydda den egna datorn mot virus.
- Om hotelsebrev kommer till brevlådan ska det ej tas bort.
- Kontoinnehavaren är skyldig att löpande ta bort inaktuella meddelanden från sin inkorg.
- Ett e-postmeddelande kan skickas till och läsas av fel adressat, var därför noggrann när du adresserar din e-post

14.10 Loggning

All distribution av e-post loggas. Vid denna loggning loggas dock inte innehållet. Däremot loggas teknisk data, mottagaradress och vilket e-postkonto som använts. Vid misstanke om brott kan loggfilerna komma att lämnas ut till rättsskipande myndighet utan att kontoinnehavaren meddelas.

Arbetsgivaren kan komma att ta del av de uppgifter som finns i ett e-postmeddelande om det är nödvändigt för att uppfylla myndighetens skyldigheter om allmänna handlingars offentlighet. Arbetsgivaren kan även komma att ta del av de uppgifter som finns i ett e-postmeddelande om det är nödvändigt vid fara för informationssäkerhet, t.ex. vid virus- och hackerangrepp, eller för att utreda och förhindra brott.

14.11 Lagring av information

Lagring och hantering av information i mobila enheter t.ex. telefoner och surfplattor ska följa Örebro kommuns Regler och Riktlinjer för Informationssäkerhet.

14.12 Ansvar

Varje användare ansvarar för att gällande riktlinjer följs. I ansvaret ingår även att till överordnad verksamhetsansvarig rapportera olika former av incidenter.

Varje verksamhetsansvarig ansvarar för att riktlinjerna hålls levande. Om hantering, som står i strid med gällande lagstiftning eller lokala föreskrifter meddelade av Örebro kommun, uppdagas är verksamhetsansvarig skyldig att vidtaga åtgärder. I ansvaret ingår även att underrätta säkerhetschefen om olika former av incidenter på det sätt som säkerhetschefen fastställt. Denna rapportering syftar till att samla in underlag om de incidenter som förekommer i kommunen.

14.13 Utbildning och information

Alla användare ska ta del av och känna till riktlinjerna och dess innebörd. Det åligger varje verksamhetsansvarig att ge användarna den information och utbildning som krävs för att kunna följa riktlinjerna innan tillträde ges till de i dessa riktlinjer uppräknade administrativa resurserna för kommunikation.