MELLERUDS KOMMUN

Riktlinjer för Informationssäkerhet

– Melleruds Kommun

Antagen av Kommunstyrelsen den
11 februari 2026, § 23
Dnr: KS-2025-00495

Kommunstyrelseförvaltningen

Postadress: 464 80 Mellerud **Besökadress:** Storgatan 11
Tfn: 0530-180 00 **E-post:** kommunen@mellerud.se
Bankgiro: 5502-2776 **Orgnr:** 212 000-1488 | **www.mellerud.se**

Inledning

Förevarande informationssäkerhetsbestämmelser är utformade att komplettera Melleruds kommuns informationssäkerhetspolicy (Dnr: XXXX) med konkreta anvisningar för Melleruds kommuns informationssäkerhetsarbete samt att ge vägledning i kommunens ledningssystem för informationssäkerhet. Samtliga nämnder samt kommunala bolag omfattas av informationssäkerhetsbestämmelserna.

Bestämmelserna är uppdelade i tre kapitel:

Kapitel	
A	Informationssäkerhet för medarbetare.
B	Styrningen av informationssäkerhet.
C	Informationssäkerhet i IT-miljön och i verksamhetsnära förvaltning.

Kapitel A: Informationssäkerhet för medarbetare

A1 Övergripande regler

Bestämmelserna i detta kapitel syftar till att tydliggöra för medarbetaren om de skyldigheter och ansvar som medföljer med att arbeta i offentlig verksamhet utefter ett informationssäkerhetsperspektiv. Detta avser ett förhållningssätt gentemot att kommunens arbete präglas av en offentlighet, ett ansvar att skydda sin digitala identitet och den IT-utrustning som kommunen erbjuder sina anställda samt att arbeta utefter en gemensam plattform för informationshantering.

A1.1 Medarbetare ansvarar för att följa de bestämmelser som fastställs i detta dokument.

A1.2 Medarbetare ska vara medveten om att den information som upprättas inom ramen för sin tjänsteutövning ska som utgångspunkt anses att vara allmän handling och kan bli föremål att vara offentlig. All datatrafik vid användning av Melleruds kommuns IT-utrustning tillhör kommunen och arbetsgivaren har under särskilda förutsättningar tillgång till det material som upprättas med kommunens digitala verktyg.

A1.3 Medarbetare ska hålla sin digitala identitets inloggningsuppgifter och koder hemliga, vara aktsam med och ta ansvar för sina digitala verktyg samt inte använda sig av privata konton eller lösenord i tjänst.

A1.4 Den IT-utrustning som tillhandahålls inom ramen för medarbetarens yrkesutövning är personlig och ska inte delas, lånas ut eller överlåtas utan godkännande från närmaste chef. Medarbetare ska låsa sin IT-utrustning när den är utanför uppsikt, såsom att logga ut från datorn och aktivera skärmlås på tjänstetelefon eller läsplatta så att ingen obehörigen kan komma åt information.

A1.5 Medarbetare ansvarar för att den information som den upprättar eller på annat sätt förfogar över i sin tjänst hanteras på ett korrekt, lämpligt och säkert sätt.

A2 Informationshantering

Informationshantering avser informationens kretslopp och livstid, allt från upprättande, lagring, gallring, hantering via e-post och utlämnande eller publicering av information.

Informationsklassning och bedömning av information

Informationsklassning avser en bedömning av kommunens informationstillgångar med ändamålet att avgöra lämpliga åtgärder i förhållande till informationens skyddsvärde.

A2.1 Information som upprättas och skickas inom organisationen ska klassas lämpligt utefter informationens innehåll och det ska framgå tydligt gentemot mottagaren. Känsligheten i ett dokument som upprättas eller i ett epostmeddelande som skickas ska markeras att vara antingen *öppen, intern eller konfidentiell*.

Öppen	Intern	Konfidentiell
Information som är öppen och offentlig. Innehåller varken känsliga eller extra skyddsvärda personuppgifter eller sekretess.	Information som är tilltänkt att vara för internt bruk. Kan innehålla personuppgifter och/eller sekretess.	Information som omfattas av sekretess eller innehåller extra skyddsvärda eller känsliga personuppgifter.

A2.2 Medarbetare ansvarar för att ha kännedom kring dataskyddsförordningens definitioner av extra skyddsvärda och känsliga personuppgifter.

A2.3 Medarbetare ska vara införstådd med kommunens informationsklassningsmodell.

Lagring och gallring

Informationshantering omfattar även behandlingsåtgärderna för hur information lagras, arkiveras eller gallras. Vid användning som är att bedöma vara av privat karaktär på den tilldelade IT-utrustningen som kommunen erbjuder, ansvarar inte kommunen för tillgänglighet eller åtkomst till filer eller nätverk.

A2.4 Information ska lagras i Melleruds kommuns beslutade lagringsplatser, i enlighet med dokumenthanteringsplanen. Medarbetarens e-post, meddelanden, dokument och filer ska gallras enligt gällande dokumenthanteringsplan.

A2.5 Varje verksamhet som handhar konfidentiell information i fysiskt format ska ha upprättade regler för hur dessa ska lagras.

A2.6 Kommunen ansvarar inte för åtkomst eller tillgänglighet av privata filer, datautrustning eller nätverk för privat bruk.

Information via e-post

Den E-post som kommer kommunen tillhanda ska hanteras på ett tryggt, förutsägbart och skyndsamt sätt. Det är av vikt att e-post utanför medarbetarens egen kommun-e-postadress, såsom funktionsbrevlådor, hanteras likformigt då kravbilden är den samma.

A2.7 Medarbetare ska inte använda sin @mellerud.se-adress för privat bruk eller vidarebefordra e-post till externa e-postadresser. E-post sänd till en @mellerud.se-adress ska besvaras med en @mellerud.se-adress.

A2.8 E-postkonton med syfte att delas med flera, såsom funktionsbrevlådor, ska ha tydligt kommunicerat ansvariga för att bevaka och administrera dessa.

Utlämnande och publicering av information

Utlämnande och publicering av information innebär att informationen skyddsvärde är att bedöma som öppen för allmänheten att ta del utav, därför är det viktigt att vara noggrann vid utlämnande av information så att informationens konfidentialitet inte röjs.

A2.9 Medarbetare ansvarar för att följa den beslutade arbetsprocessen vi begäran om allmän handling.

A2.10 Medarbetare ansvarar för att följa de beslutade rutinerna för publicering på internet i Melleruds kommuns namn.

A3 Distansarbete

Distansarbete avser arbete på annan plats än vad som är beslutad ordinarie arbetsplats. Arbete utanför ordinarie beslutad arbetsplats växer sig till ett vanligare arbetssätt för medarbetare i Melleruds kommun. Trots ökad flexibilitet och frihet, ställer detta dock högre krav på hur medarbetaren ska hantera information som den förfogar över i tjänsten.

A3.1 Medarbetare ansvarar för att följa kommunens informationssäkerhetspolicy och informationssäkerhetsbestämmelser på samma sätt distans som på ordinarie arbetsplats.

A3.2 Om medarbetare ska arbeta på distans ska förutsättningarna klargöras i överenskommelse med närmaste chef, till exempel vilken plats som avses vara utsedd distansarbetsplats samt vilka arbetsuppgifter som inte är lämpliga att utföra på avsedd distansarbetsplats.

A3.3 Medarbetare ansvarar för att obehöriga inte kan ta del av arbetsmaterial, intern eller konfidentiell information i samband vid distansarbete.

A4 Säkerhetsmedvetande

Säkerhetsmedvetandet i förhållande till informationssäkerhet avser bland annat kunskapshöjande insatser för ämnesområdet informationssäkerhet, att etablera en hållbar säkerhetskultur där misstag är mänskligt samt att brister och avvikelser i kommunen rapporteras som gör att vi lär oss och utvecklas tillsammans. Ändamålet är att kommunen ska bli en tryggare plats att arbeta och leva i.

Det är av yttersta vikt att samtliga medarbetare i kommunen hjälper kommunens IT-avdelning att rapportera misstänka E-postmeddelanden samt länkar och filer då medarbetaren är Melleruds kommuns yttersta skyddslager.

A4.1 Intern och konfidentiell information ska alltid kommuniceras på ett sätt så att ingen obehörig kan ta del informationsutbytet.

A4.2 Den information och de uppgifter som den anställde får tillgång till i tjänsten ska hanteras med försiktighet. Vid samarbete med andra ska information minimeras till vad som är att bedöma nödvändig för att utföra sina arbetsuppgifter. Vid osäkerhet ska den anställde vända sig till sin närmaste chef för vägledning.

A4.3 Medarbetare är skyldig att genomföra de kompetenshöjande utbildningar inom informationssäkerhet och dataskydd som Melleruds kommun tillhandahåller.

A4.4 Medarbetare ska rapportera in incidenter, avvikelser eller brister kopplade till Melleruds kommuns informationssäkerhet skyndsamt. Anmälan ska göras via ett anmälningsformulär på kommunens intranät samt att närmaste berörda chef ska underrättas om situationen. Personuppgiftsincidenter ska rapporteras till närmaste informationssäkerhetshandläggare och till kommunens dataskyddsombud skyndsamt. Vid bedömning ska sedan incidenten rapporteras till Integritetsskyddsmyndigheten inom 72 timmar från dess att incidenten upptäcktes.

A4.5 Medarbetare ska vid misstanke om virus, spam eller nätfiske, eller vid inträffad händelse, skyndsamt anmäla detta till kommunens IT-support.

Kapitel B: Styrning av informationssäkerhet

B1 Styrdokument inom informationssäkerhet

Melleruds kommun har tre nivåer av styrdokument i förhållande till informationssäkerhet:

- **Informationssäkerhetspolicy** beskriver kommunens övergripande viljeriktningar och metoder för Melleruds kommuns gemensamma informationssäkerhetsarbete. Detta styrdokument fastställs av kommunfullmäktige och ska granskas och revideras vid behov eller senast i samband med varje ny mandatperiod.

- **Informationssäkerhetsbestämmelser** är tillämpningsregler för informationssäkerhetspolicyn. Detta dokument fastställs av Kommunstyrelsen och ska granskas och revideras vid behov eller senast i samband med revisionen av Informationssäkerhetspolicyn.

- **Rutiner/instruktioner inom informationssäkerhet** kan vara kompletterande dokument till informationssäkerhetsbestämmelserna eller vara unika dokument för varje nämnd med utgångspunkt från informationssäkerhetsbestämmelserna och informationssäkerhetspolicyn. Rutiner eller instruktioner ska fastställs av respektives nämnd där de upprättas.

B1.1 Informationssäkerhetsbestämmelser måste vara förenliga med och får inte stå i strid med Melleruds kommuns informationssäkerhetspolicy.

B1.2 Rutinbeskrivningar/instruktioner inom informationssäkerhetsområdet måste vara förenliga med och får inte stå i strid med Melleruds kommuns informationssäkerhetspolicy och informationssäkerhetsbestämmelser.

B1.3 Samtliga styrdokument, rutiner och instruktioner ska vara tydligt kommunicerade på kommunens intranät och ska granskas, uppdateras och förbättras vid behov.

B2 Rollfördelning för informationssäkerhetsarbetet

Politiskt och organisatoriskt ansvar

Kommunfullmäktige antar Melleruds kommuns informationssäkerhetspolicy.

Kommunstyrelse har det högsta strategiska ansvaret för kommunens systematiska informationssäkerhetsarbete samt uppföljning av tillämpandet. Kommunstyrelsen antar informationssäkerhetsbestämmelser.

Nämnd är personuppgiftsansvarig för de personuppgifter som behandlas inom nämnden. Varje nämnd kan vid behov besluta om rutiner och instruktioner som förtydligar och kompletterar de centrala styrdokumenten inom informationssäkerhet.

IT-avdelningen ansvarar för driften av kommunens IT-infrastruktur och fungerar som stöd för kommunens övergripande verksamhet för att förse kommunens med en tillförlitlig datortekniskmiljö samt support. Melleruds kommuns IT-avdelning är ansvariga för att utveckla och förvalta IT-säkerhetsarbetet samt stödja kommunens verksamheter i dess digitaliseringsprocess.

Särskilda ansvarsroller

B2.1 Alla yrkesroller som kan kopplas till informationssäkerhet i Melleruds kommun ska vara tydligt kommunicerade och definierade inom organisationen.

Informationssäkerhetssamordnare har det strategiska ansvaret att utveckla och samordna Melleruds kommuns informationssäkerhetsarbete. Rollen ansvarar även för att genomföra revisioner inom informationssäkerhet för kommunens räkning till Kommundirektörens ledningsgrupp.

Säkerhetschef är ansvarig för organisation och ledning av krisberedskap, författningsskydd, demokratiskydd, skydd mot våldsbejakande extremism, brottsförebyggande åtgärder, säkerhetsskydd samt informationssäkerhet.

Dataskyddsombud ansvarar för att ganska efterlevnaden av dataskyddsförordningen i Melleruds kommuns nämnder. Dataskyddsombudet ansvarar för att rapportera brister och förbättringsåtgärder till respektive nämnd och till kommundirektörens ledningsgrupp.

Informationssäkerhetshandläggare är en roll som ska finnas inom varje nämnd och som ska fungera som kontaktperson till kommunens dataskyddsombud och informationssäkerhetssamordnare in till sina respektive nämnder. Informationssäkerhetshandläggarna ansvarar för att dokumentera sin nämnds behandling av personuppgifter i en registerförteckning, hjälpa till med informationsklassningar i sin nämnd samt finnas som stöd vid genomförande av kommunens informationssäkerhetsanalyser.

Kommunarkivarie har tillsynsansvar för att information i Melleruds kommun hanteras enligt bestämmelserna i tryckfrihetsförordningen, arkivlagen och offentlighets- och sekretesslagen.

Användare är den som nyttjar kommunens informationstillgångar och/eller IT-utrustning inom ramen för sin anställning eller sitt uppdrag, oavsett om individen i fråga är inhyrd konsult, entreprenör, praktikant eller anställd.

B3 Informationsklassning

En central aspekt av informationssäkerhet är att systematiskt informationsklassa information. All information som behandlas i Melleruds kommun bör inte ha samma skyddsvärde då det finns information som är mer skyddsvärd än annan och där det måste vidtas ytterligare skyddsåtgärder.

B3.1 All information ska klassificeras utefter dess känslighet för att utforma lämpliga skyddsåtgärder. Detta förfarande gäller oavsett om informationen är digital media, fysiska dokument eller muntlig.

Känsligheten ska vid utformande av dokument och e-post klassas utefter följande tre känslighetsbedömningar: Öppen, intern och konfidentiell.

B3.2 Melleruds kommun ska ha en antagen informationsklassningsmatris.

B3.3 Melleruds kommun ska ha en upprättad instruktion som avser vägledning med lagring av information i de lagringsmöjligheter som Melleruds kommun har att tillgå.

B3.4 Varje verksamhet som handhar konfidentiell information i fysiskt format ska ha upprättade regler för hur dessa ska lagras.

B3.5 Vid uppfattning om information eller informationstillgångar som faller under, eller som kan komma att falla under, säkerhetsskyddslagen (2018:585) ska verksamheten kontakta Melleruds kommuns säkerhetsskyddschef skyndsamt.

B4 Personalsäkerhet

Personalsäkerheten avser att säkerställa att medarbetare, konsulter eller leverantörer är lämpade för den roll de är tilltänka att utföra utefter en säkerhetssynpunkt. En nyanställd i kommunen ska erhålla nödvändig information och utbildning för hur kommunen arbetar med informationssäkerhet.

B4.1 För de tjänster som arbetar med information som är extra säkerhetskänsligt eller deltar i sådan verksamhet ska dessa tjänster vara placerade i säkerhetsklass och den som ska vara anställd i denna tjänst ska genomgå en säkerhetsprövning i enlighet med säkerhetsskyddslagen (2018:585). Kommunens säkerhetsskyddschef ansvarar för rutiner för säkerhetsklassning av tjänster.

B4.2 Medarbetare ska vid nyanställning omfattas av tystnadsplikt. Tystnadsplikt regleras i bilagan till anställningsavtalet. I de fall verksamheter behöver teckna särskilda, ska dessa tecknas separat.

B4.3 Det ska finnas rutinbeskrivningar vid nyanställning av personal för hur medarbetare ska förhålla sig till informationssäkerhet. Vid avslutande av anställning ansvarar medarbetare för att rådgöra med närmaste chef för vilken information som ska sparas.

B4.4 Vid nyanställning ska medarbetare ha genomgått en intern utbildning inom informationssäkerhet.

B5 Riskhantering

Varje nämnd ska vid förändrad eller ny informationshantering genomföra en riskhanteringsprocess i förhållande till informationssäkerhet och innan en ny leverantör anlitas för att behandla en nämnds information ska leverantörens informationssäkerhet granskas och kravställas.

B5.1 Melleruds kommun ska ha en beslutad riskhanteringsprocess för hur kommunen kravställer informationssäkerhet i samband med upphandlingar av nya informationssystem. Riskhanteringsprocessen ska genomföras i samband vid införande av nya arbetsprocesser där det förekommer ny behandling av personuppgifter vid redan upphandlade informationssystem.

B5.2 Informationsägaren är ansvarig att riskhanteringsprocessen följs och för att en tillräcklig kravställan av en leverantör sker innan en upphandling slutförs.

B5.3 Informationssäkerhet och dataskydd ska beaktas vid kommunens IT-råd och ska representeras av nämndens utsedda informationssäkerhetshandläggare.

B5.4 Vid fall där en leverantör ska behandla personuppgifter åt en nämnd ska det tecknas ett personuppgiftsbiträdesavtal med leverantören.

B5.5 Vid fall där IT-kravställningen eller IT-säkerheten inte anses vara tillräckliga, eller utrett tillräckligt, vid en upphandling har kommunens IT-chef möjlighet att stoppa eller pausa upphandlingen.

B5.6 Vid fall där informationssäkerheten inte anses vara tillräcklig, eller utrett tillräckligt, vid en upphandling har kommunens säkerhetschef möjlighet att stoppa eller pausa upphandlingen.

B6 Incidenthantering

Incidenthantering avser hanteringen av en händelse som är av avvikande karaktär där utredningen har till avsikt att mynna ut i lärdomar från den inträffade händelsen. Det ska finnas en intern funktion för att genomföra rapportering och det ska finnas rutiner för hanteringen av dessa rapporteringar.

B6.1 Melleruds kommun ska ha rutiner för hur en informationssäkerhetsincident ska rapporteras samt tillhandahålla en intern funktion för att genomföra inrapporteringar. Tydliga roller och ansvar ska finnas för hanteringen av informationssäkerhetsincidenter. Alla informationssäkerhetsincidenter ska dokumenteras.

B6.2 Det ska finnas dokumenterade rutiner för incidentrespons för informationssäkerhetsincidenter.

B7 Registerförteckning och den registrerades rättigheter

I enlighet med dataskyddsförordningen ska varje organisation föra och ha upprättade register över de processer som innehåller personuppgiftsbehandlingar. I Melleruds kommun medför detta att respektive nämnd ska ha en egen upprättad och uppdaterad registerförteckning.

B7.1 Varje nämnd ska ha en uppdaterad registerförteckning över sina behandlingsprocesser och system.

B7.2 Registrerade ska informeras hur Melleruds kommun behandlar deras personuppgifter. Melleruds kommun ska således ha en extern informationstext på Melleruds hemsida samt en intern informationstext på intranätet.

B7.3 Den registrerade ska ha rätt till:

- Tillgång att få en kopia på begäran av dennes personuppgifter som behandlas av Melleruds kommun.
- Att bli glömd, när detta förfarande kan anses tillämpbart.
- Dataportabilitet, när detta förfarande kan anses tillämpbart.
- Att göra invändningar eller begränsa behandlingen, när detta förfarande kan anses tillämpbart.

B7.4 Begäran om registrerades rättigheter ska fullgöras inom en månad. Undantag måste ha berättigade skäl.

B7.5 Innan en begäran om rättigheter kan åtas måste den registrerade identifiera sig.

B8 Intern revision

Melleruds kommuns informationssäkerhetssamordnare och dataskyddsombud har till uppgift att initiera granskningar i förhållande till kommunens informationssäkerhetsarbete och dataskyddsombudet har som särskild uppgift att granska efterlevnaden av dataskyddslagstiftning.

B8.1 Informationssäkerhetssamordnaren ska avrapportera Melleruds kommuns informationssäkerhetsarbete varje år till kommundirektörens ledningsgrupp och samtliga nämnder.

B8.2 Vartannat år ska en större informationssäkerhetsanalys genomföras och presenteras till kommundirektörens ledningsgrupp. Särskilda skäl, exempelvis allvarliga incidenter, brister eller behov, kan motivera ytterligare rapporteringar.

B8.3 Melleruds kommuns dataskyddsombud ska avrapportera dataskyddsarbetet vid samtliga nämndsmöten halvårsvis. Vid behov lyfts frågan till kommundirektörens ledningsgrupp på begäran av dataskyddsombudet.

B9 Internet och sociala medier

Eftersom Melleruds kommun har en webbplats och är aktiv i sociala medier ska det finnas rutinbeskrivningar som reglerar användandet av dessa tjänster.

B9.1 Det ska finnas rutinbeskrivningar som reglerar skapande av information på Melleruds kommuns sociala medier.

B9.2 Varje förvaltning ska ha egenupprättade rutiner som reglerar diarier, kallelser och hur protokoll publiceras på mellerud.se.

B9.3 Det ska finnas rutinbeskrivningar som reglerar hur personuppgifter publiceras på mellerud.se.

B10 Bevarande, gallring och utlämnande av allmänna handlingar

Melleruds kommun ska ha rutiner och instruktioner för hur kommunen ska hantera allmänna handlingar, såsom vid bevaring, gallring och utlämnande av dessa. Dessa rutiner ska också finnas tillgängliga för samtliga medarbetare.

B10.1 Varje nämnd ska ha en upprättad dokumenthanteringsplan som beskriver myndighetens handlingar och beslutade gallringsfrister. Dokumenthanteringsplanen ska vara kommunicerad inom nämnden.

B10.2 Varje nämnd ska ha en utsedd arkivansvarig som ansvarar för att dokumenthanteringsplanen är uppdaterad och korrekt.

B10.3 Det ska finnas en rutinbeskrivning för utlämnande av allmänna handlingar som följer offentlighets- och sekretesslagen.

Kapitel C: Informationssäkerhet i IT-miljön och i verksamhetsnära förvaltning

Detta kapitel reglerar informationssäkerheten i utveckling, verksamhetsdrift och förvaltning av Melleruds kommuns IT-miljö.

C1 Roller och ansvar i den verksamhetsnära förvaltningen

Informationsägare har det övergripande och yttersta ansvaret för informationen. Informationsägaren ansvarar för att klassa information enligt Melleruds kommuns klassningsmodell och avgöra på vilket sätt informationen får behandlas. Informationsägaren är ansvarig för riskhanteringsprocessen i samband med informationssäkerhetskravställningen vid en upphandling.

Systemägare har det övergripande ansvaret för respektive system och dess användning. Utsedd systemägare kan därtill vara informationsägare av informationen som finns i systemet.

Systemförvaltare har det dagliga ansvaret för ett system. Systemförvaltaren fungerar i hög grad som systemägarens utförare och ser till att systemets funktionalitet samt beslutade aktiviteter genomförs och upprätthålls.

Systemadministratör har det dagliga ansvaret för administrationen av systemet. En och samma person kan ha båda rollerna systemförvaltare och systemadministratör.

Driftförvaltare bistår systemförvaltaren vid felavhjälpning, installation av uppdateringar samt paketering och distribution av klientprogramvara. Driftförvaltaren kan ha uppdraget att övervaka loggfiler, generell databasvård och se till att backuper inhämtas enligt överenskommelse.

Digitala coacher bistår kollegor i verksamheten med att införa olika digitala system och hjälpmedel. Arbetar också med att upptäcka och lyfta potentiella risker gällande informationssäkerheten.

C1.2 Roller för digitaliserade processer

Processägare är ansvarig för att processen uppfyller funktionalitet enligt verksamhetens behov. Processägaren utses av förvaltningschef eller motsvarande och i de fall en process saknar processägare ansvarar förvaltningschef eller motsvarande för denna roll tills en processägare utses. Processägarens ansvar kan inte delegeras till annan roll inom processförvaltningen.

Processförvaltare har det övergripande ansvaret med den dagliga administrationen av processen utifrån processägarens mål.

E-tjänstutvecklare ansvar för att tillsammans med verksamheten skapa, förvalta och vidareutveckla digitala processer utifrån verksamhetens behov samt utvecklingsverktygets förutsättningar. E-tjänstutvecklaren ansvar för systemförvaltning och utveckling av e-tjänsteplattformen. I detta ansvar ingår att informera processförvaltaren om planerade driftstopp samt hantera kontakten med IT-avdelningens driftförvaltare och leverantören av utvecklingsverktyget vid uppdateringar och eventuella fel och brister i systemet.

C2 Informationssäkerhet i IT-förvaltningen

För att säkerställa informationssäkerheten i IT-förvaltningen är det viktigt att det finns en struktur i syfte att skydda den information som finns inom dessa verksamhetsgrenar.

Övergripande administrering

C2.1 Det ska finnas dokumentation av Melleruds kommuns IT-system som beskriver IT-miljön och därtill en process för att regelbundet uppdatera denna dokumentation.

C2.2 Kritiska IT-resurser som servrar, operativsystem, verksamhetsapplikationer, brandväggar, routers och switchar ska härdas enligt branschstandard.

C2.3 Fysiska ingrepp, såsom modifiering av hårdvara, får enbart utföras av Uddevalla kommuns IT-avdelning eller av annan av IT-avdelningen utsedd medarbetare vid kommunen.

C2.4 Melleruds kommun ska ha rutiner för återlämning av IT-utrustning, återställning och hantering av den återlämnande IT-utrustningen.

Personalsäkerhet

C2.5 Samtliga IT-medarbetare i Melleruds kommun med höga behörighet till kritiska system ska vara lämpliga ur en säkerhetsbakgrund. Därför ska dessa medarbeta genomgå bakgrundskontroll eller i särskilda fall säkerhetsprövning.

C2.6 Den tilldelade behörigheten är tidsbegränsad och är kopplad till anställning, projektdeltagande eller uppdrag. Användaren skall själva meddela omständigheter som medför att behörigheten skall upphöra.

Nätverksregler och åtkomstkontroll

C2.7 Melleruds kommun ska följa zero-trust-modellen i organisationen datatekniska miljö enligt branschstandard.

C2.8 Melleruds kommun ska granska brandväggars- och routers regeluppsättningar rutinmässigt.

C2.9 Samtliga användare i Melleruds kommun ska vara försedda med en unik användaridentitet.

C2.10 Åtkomst till IT-system ska hanteras enligt händelsefall och Melleruds kommun ska sträva efter en automatisk identitetshantering.

C2.11 Medarbetare ska bara ha behörigheter i den grad som är nödvändigt för att fullgöra sina arbetsuppgifter och inte ha åtkomst till mer information än vad som rör individens arbetsuppgifter.

C2.12 Det ska finnas en dokumenterad och regelbundet uppdaterad åtkomstkontrollista som definierar roller, befattningshavare och behörighet till informationssystem inom Melleruds kommun. Systemägare ska ge godkännande innan behörigheter ges ut till personal. Samtliga förändringar i roller eller behörigheter i system ska rapporteras till IT-avdelningen.

C2.13 Användaridentiteten ska alltid kunna spåras, därför är det inte tillåtet att använda annan

användares behörighet eller utnyttja felaktiga konfigurationer, programfel eller på annat sätt manipulera IT-resurserna. Gruppkonton får inte förekomma i verksamhetskritiska system.

Kryptografi-, och logghantering

C2.14 Algoritmer som används för kryptering ska vara starka och industriaccepterade och hantering av krypteringsnycklar ska genomföras enligt gällande best practice. All konfidentiell information ska lagras krypterat.

C2.15 Vid verksamhetskritiska system ska loggar finnas för att säker ställa spårbarheten vid förmågan att rekonstruera säkerhetshändelser. Loggar från verksamhetskritiska system ska ha möjlighet att centralt hanteras i IT-avdelningens loggsystem. Loggar ska bevaras enligt rutin och med begränsad åtkomst

Hantering av tekniska sårbarheter

C2.16 Hantering av upptäckta sårbarheter i Melleruds kommuns IT-miljö ska hanteras omgående och IT-chef har mandat att vidta de åtgärder som är nödvändiga för att hantera den upptäckta sårbarheten.

C2.17 Säkerhetspatchar installeras enligt givet schema samt enligt best practice.

C2.18 Melleruds kommun ska ha en beskrivning av sin datortekniska miljö som ska uppdateras regelbundet när det sker större förändringar.

C2.19 Melleruds kommun ska ha en avbrottsplan och som ska testas regelbundet.

C2.20 Melleruds kommun ska regelbundet omvärldsbevaka för att leta efter nya sårbarheter inom IT, därefter agera proaktivt och arbeta för att minimera större kostnader, avbrott eller informationssäkerhetsincidenter i framtiden.

C3 Informationssäkerhet i IT-utvecklingen

Melleruds kommun ska i sin digitaliseringsprocess beakta informationssäkerhet som ett centralt inslag vid vidareutveckling av kommunens digitala miljö.

Säker utveckling

C3.1 Principen om ”inbyggt dataskydd” och ”dataskydd som standard” från GDPR ska efterlevas.

C3.2 Utvecklings-, test- och produktionsmiljöer ska vara skilda från varandra genom logisk eller fysisk separation. Testkonton ska alltid raderas från system när de sätts i produktion.

C3.3 Utvecklare ska ha begränsade behörigheter i produktionsmiljöer där det finns skyddsvärd eller säkerhetskänslig information.

C3.4 Konfidentiell information får inte användas i test- eller utvecklingssyften.

C3.5 Vid utveckling av webbapplikationer ska råden från OWASP Top 10 beaktas.

Ändringshantering

C3.6 Ändringar i verksamhetskritiska system måste genomgå en formell ändringshanteringsprocess.

C3.7 Vid avveckling av system ska det finnas dokumenterade rutiner för hur informationen i det avvecklade systemet ska migreras, destrueras eller arkiveras.

Kontinuitetshantering

C3.8 Det ska finnas en formell, dokumenterad kontinuitetsplan som kan tillämpas på verksamhetskritiska system med hög tillgänglighetsklassning. Kontinuitetsplaner ska testas regelbundet