Österbottens välfärdsområde
Pohjanmaan hyvinvointialue

Datasäkerhetspolicy

Österbottens välfärdsområde

Styrelsen 16.1.2023 § xx

Träder i kraft 1.1.2023

Innehållsförteckning

Österbottens välfärdsområdes datasäkerhetspolicy

1. Inledning

Österbottens välfärdsområde tillhandahåller sina tjänster utgående från kundernas behov. Tillhandahållandet av tjänsterna bygger på information och behandling av information i Österbottens välfärdsområdes miljö. Välfärdsområdets serviceproduktion är avhängig av IKT-teknik samt obrutna och säkra IKT-tjänster.

Österbottens välfärdsområdes strategi ”Nära människan, innovativt och på två språk” utkristalliseras i serviceattityden ”Hej, hur kan jag hjälpa dig”. Måluppfyllelsen förutsätter en omfattande digitalisering men också att alla delområden som anknyter till datasäkerhet, helhetsarkitektur och kompatibilitet tas i beaktande redan i planeringsskedet och sedan kontinuerligt.

I denna datasäkerhetspolicy definieras de principer, mål, ansvarsfrågor och tillvägagångssätt som hänför sig till den datasäkerhet som omfattar ledningen, tjänsterna och verksamheten i Österbottens välfärdsområde. Datasäkerhetspolicyn fungerar som grund för alla andra anvisningar som hänför sig till datasäkerhet och i vilka man preciserar de bestämmelser som fastställs i denna datasäkerhetspolicy och utgående från vilka man utfärdar direktiv om hur dessa ska omsättas i praktiken.

Datasäkerhetspolicyn berör välfärdsområdets organisation, dess anställda och förtroendevalda samt representanter för Österbottens välfärdsområdes intressegrupper som i deras arbete eller inom ramen för deras uppdrag behandlar information som ägs eller förvaltas av Österbottens välfärdsområde. Datasäkerhetspolicyn omfattar all information i Österbottens välfärdsområde oberoende av framställningssätt, form, skyddsnivå eller livscykelfas.

2. Relevans för organisationen

De organisationsförändringar som gjorts den senaste tiden, såsom social- och hälsovårdsreformen, och de lagstiftningsförändringar som gjorts under den senaste tiden, såsom Europeiska unionens tillgänglighetsdirektiv och allmänna dataskyddsförordning samt den nationella dataskyddslagen, syftar till att säkerställa att datasäkerhet, dataskydd, riskbedömning, helhetsarkitektur och kompatibilitet tas i beaktande i planering för att man därigenom ska kunna uppnå kostnadsbesparingar och främja användbarheten av informationen.

För att datasäkerheten ska kunna omsättas i praktiken måste välfärdsområdet både identifiera de tjänster som är livsviktiga för områdets verksamhet och fastställa tillräckligt omfattande

datasäkerhets principer för att trygga dessa tjänster. För att bidra till datasäkerheten har Österbottens välfärdsområde i bland annat datasäkerhetsplanen, datasäkerhetspolicyn samt anvisningarna om intern kontroll och riskhantering fastställt tillvägagångssätt och anvisningar som hänför sig till datasäkerhet.

3. Definition

Datasäkerheten omfattar de ansvar och den praxis som hänför sig till datasäkerhet och dataskydd, vilka syftar till att säkerställa att uppgifter, datasystem och tjänster skyddas och säkras så att man kan säkerställa och påvisa deras konfidentialitet, integritet och tillgänglighet.

- **Konfidentialitet** (confidentiality): Det här avser de åtgärder som används för att identifiera konfidentiell information och trygga dess konfidentialitet. Det vill säga att enbart behöriga personer har tillgång till uppgifter, datasystem och tjänster, samtidigt som man ser till att dessa inte röjs eller på annat sätt görs tillgängliga för obehöriga.
- **Integritet** (integrity): Det här avser de åtgärder som används för att säkerställa att uppgifter är riktiga, obrutna och förvaras i adekvat tid. Det vill säga att uppgifterna, datasystemen och tjänsterna är riktiga och obrutna, eller inte har förändrat till följd av avsiktlig eller oavsiktlig teknisk eller mänsklig verksamhet.
- **Tillgänglighet** (availability): Det här avser de åtgärder som används för att trygga att uppgifter kan användas på korrekt sätt. Det vill säga att uppgifter, datasystem och tjänster vid behov ohindrat kan användas av behöriga personer. Med passagekontroll säkerställer man att uppgifter eller datasystem inte kan användas utan tillåtelse. Genom autentisering säkerställer man att parter blir tillförlitligt identifierade.

Dataskyddsrelaterade frågor behandlas mer i detalj i Österbottens välfärdsområdes dataskyddspolicy.

4. Åligganden som styr

Datasäkerheten i Österbottens välfärdsområde förpliktas och styrs av allmänna lagstadgade åligganden samt verksamhetsspecifika ålägganden i speciallagstiftning. Men också av övriga åligganden, bestämmelser och anvisningar som hänför sig till datasäkerhet, såsom säkerhetsavtal som ingåtts med leverantörer. Därtill tillämpas övriga anvisningar som hänför sig till datasäkerhet till tillämpliga delar (bl.a. JUHTA/VAHTI). Klient- och patientuppgifter som omfattas av lagstadgad arkiveringsskyldighet arkiveras och lagras vederbörligt i enlighet med arkivverkets kriterier och SÄHKE 2-kriterierna. Datasäkerhetsplanen styrs av THL:s rekommendationer. Organisationen stöds dessutom av många offentliga aktörer inom social-

och hälsovårdsbranschen, såsom dataombudsmannen, social- och hälsovårdsministeriet, myndigheten för digitalisering och befolkningsdata och finansministeriet.

Österbottens välfärdsområdes högsta ledning har till uppgift att på strategisk nivå styra utvecklandet av datasäkerheten tillsammans med informationsförvaltningen och övriga aktörer som ansvarar för datasäkerheten.

5. Ledning och ansvar

Direktören för Österbottens välfärdsområde ansvarar för datasäkerheten. Det operativa ledningsansvaret innehas av IT-direktören. Datasäkerhetsrelaterade styrdokument behandlas i den regionala IKT-styrgruppen och tas till styrelsen för godkännande.

Ansvaret för utvecklandet och övervakningen av datasäkerheten samt främjandet av medvetenheten om datasäkerheten bärs i Österbottens välfärdsområde av IT-direktören, inom ramen för de befogenheter och resurser som ledningsgrupperna tilldelat hen.

Varje person som behandlar uppgifter, upprätthåller eller använder datasystem eller datanät i Österbottens välfärdsområde är i sista hand ansvarig för att hon eller han efterlever de krav som fastställts för datasäkerheten. I Österbottens välfärdsområde ansvarar varje ägare av datasystem och ägare av de uppgifter som finns i dessa datasystem för att deras uppgifter och datasystem är skyddade. I Österbottens välfärdsområdes datasäkerhetsplan finns en detaljerad beskrivning av dessa ansvarsfrågor.

6. Utbildning

Förverkligandet av datasäkerheten bygger på denna skriftliga datasäkerhetspolicy som godkänts av ledningen för Österbottens välfärdsområde. Respektive anställd och användare av datasystem i Österbottens välfärdsområde ges anvisningar som baserar sig på denna policy. Anvisningarna som är till för anställda och användarna av datasystem finns på Österbottens välfärdsområdes intranät. Datasäkerhetspolicyn finns också på Österbottens välfärdsområdes intranät.

Den måluppfyllelse som fastställts för datasäkerheten är en oavbruten process som inrymmer administrativa, fysiska och tekniska lösningar.

Varje anställd i Österbottens välfärdsområde, vars uppgifter förutsätter förtrogenhet med datasäkerhetsanvisningarna upplyses om var de finns samt hur datasäkerheten är organiserad i Österbottens välfärdsområde.

Alla anställda har tillgång till datasäkerhetsanvisningarna i och med att de finns på välfärdsområdets intranät på adressen intra.pohjanmaanhyvinvointi.fi

De som ansvarar för upprätthållandet, utvecklandet och ledningen av datasäkerheten ska också erbjudas möjlighet till tillräcklig grundutbildning och vidareutbildning. Utbildningsbehovet utvärderas årligen av ledningen för informationsförvaltningen.

7. Datasäkerhetsplan

Datasäkerhetspolicyn ligger till grund för Österbottens välfärdsområdes datasäkerhetsplan samt de dataskyddsanvisningar som är till för användare, IT-ansvariga och informationsförvaltningen.

Österbottens välfärdsområde använder sig av en säkerhetsklassificering av uppgifter och datasystem. Respektive säkerhetsklass har en fastställd datasäkerhetsnivå och fastställda åtgärder som vidtas för att trygga den fastställda datasäkerhetsnivån. Varje datasystem ska ha en ägare. Ett register upprätthålls över systemens ägare.

Anställda delges de datasäkerhetsanvisningar som de behöver i sin verksamhet och datasäkerheten är en del av den allmänna introduktionen. Vikarier, studerande och samarbetsparter informeras om datasäkerheten samt de regler och rekommendationer som gäller dem. Österbottens välfärdsområdes anställda utbildas i datasäkerhet genom meddelanden via olika kommunikationskanaler och genom utbildningstillfällen. Nivån på den datasäkerhet som anknyter till databehandlingen och datasystemen i Österbottens välfärdsområde bedöms med de medel som den interna kontrollen förfogar över, och vid behov även med hjälp av extern revision. Brister i datasäkerhet analyseras tillsammans med dem som upprätthåller och äger systemen.

Välfärdsområdet säkerställer också att serviceproducenter genom avtal förbinder sig till att det system eller den tjänst som upphandlas för behandling av uppgifter uppfyller kraven på inbyggt dataskydd och dataskydd som standard. Den personuppgiftsansvariges skyldigheter och den registrerades rättigheter beaktas redan då informationssystemet definieras och tas i bruk.

8. Datasystem

De apparater, program, datasystem och uppgifter som Österbottens välfärdsområde överlåtit till anställda är avsedda för skötseln av arbetsuppgifter. I Österbottens välfärdsområdes datasystemmiljö får man bara använda datasystem, apparater och program som godkänts av styrelsen och informationsförvaltningen. Installationsarbeten utförs av 2M-IT eller aktörer som är i avtalsförhållande till Österbottens välfärdsområde, såsom IKT-serviceleverantörer samt system- och apparatleverantörer. I avtal mellan välfärdsområdet och dylika aktörer ska de ansvarsfrågor och åligganden som hänför sig till datasäkerhet och dataskydd tas i beaktande.

9. Användning av datasystem

Varje anställd i Österbottens välfärdsområde förbinder sig att hantera uppgifter och datasystem på ett datasäkert sätt och enligt givna anvisningar genom att underteckna en förbindelse. Likaså förutsätts Österbottens välfärdsområdes förtroendevalda, som ges rätt att använda datasystem som ägs av Österbottens välfärdsområde, underteckna denna förbindelse.

Datasystem som ägs av Österbottens välfärdsområde identifieras, samtidigt utses en organisationsenhet till ägare som ansvarar för hanteringen av de befogenheter som hänför sig till ifrågavarande datasystem.

Det datasäkra tillvägagångssättet beskrivs noggrannare i datasäkerhetsanvisningarna. Försummelser och oegentligheter hanteras utan dröjsmål.

10. Klassificering av uppgifter

Uppgifter som ägs av Österbottens välfärdsområde klassificeras av den som äger informationen. Klassificeringen av uppgifter baserar sig på lagen om offentlighet i myndigheternas verksamhet (offentlighetslagen, 621/1999) samt noggrannare anvisningar som Österbottens välfärdsområde avgett om tillämpningen av denna lag. Enligt offentlighetslagen är dessa klasser: offentlig, icke-offentlig och sekretessbelagd.

Vid användning av molntjänster bör man ta i beaktande att oklassificerad information inte får laddas upp i molnet.

11. Kommunikation

Personalen informeras om aktuella datasäkerhetsrelaterade frågor och anvisningar samt avvikande lägen i regel per e-post och via närchefen. Varje närchef är ålagd att följa med och säkerställa att anställda tar del av dylika meddelanden.

Vid upprättandet av serviceavtal med utomstående IKT-serviceleverantörer av teknisk datasäkerhet (t.ex. virusskydd, brandmurar och filtrering av skräppost) ska man skriftligen komma överens om vem som ska kontaktas och vem som ansvarar för kommunikationen i samband med avvikande lägen.

12. Riskhantering

Hanteringen av datasäkerhetsrisker bygger på identifiering och konsekvensanalyser samt beslut om vilka åtgärder som ska vidtas för att hantera dylika risker. I Österbottens välfärdsområde dimensioneras skyddsåtgärderna utgående från riskerna i samråd med den som äger informationen och informationsförvaltningen.

13. Resiliens, kontinuitet och återställning

De objekt som ska skyddas i datasystem och tjänster som används i Österbottens välfärdsområde måste fastställas och beskrivas. Dessutom måste de objekt som ska skyddas prioriteras.

Resiliensen i verksamheten uppstår genom åtgärder som vidtas i syfte att utveckla datasäkerheten i organisationen, och här utgör säkerställandet av kontinuiteten en viktig del. Säkerhetskopior av datasystem ska testas och deras drift måste säkerställas genom simulerade störningssituationer. Kontinuitetsplanen uppdateras årligen.

Med återställning avses organisationens förmåga att återhämta sig efter störningssituationer. De roller och arrangemang som hänför sig till reservpersonal och reservsystem samt användningen av ersättande program måste säkerställas för att verksamheten inte ska drabbas av oförutsedda förändringar i samband med störningar.

14. Främjande av datasäkerhet

Det operativa utvecklingsansvaret innehas av IT-direktören. Datasäkerhetsrelaterade styrdokument behandlas i IKT-styrgruppen och tas till styrelsen för godkännande.

I Österbottens välfärdsområde ansvarar IT-direktören inom ramen för de befogenheter och resurser som styrelsen tilldelat hen för utvecklandet och övervakningen av datasäkerheten samt främjandet av medvetenheten om datasäkerheten.

Österbottens välfärdsområdes högsta ledning har gett IT-direktören befogenhet och skyldighet att kartlägga datasäkerheten i välfärdsområdets datasystem och vidta åtgärder för att korrigera de svagheter som hen upptäcker i datasäkerheten.

Datasäkerhetsarbetet i Österbottens välfärdsområde bygger på en ständig utveckling av verksamheten, teknologin och kompetensen i linje med följande principer:

PLANERING – Välfärdsområdets styrelse och de som ansvarar för datasäkerheten upprättar policyn, principer och planer på basis av analyser och bedömningar. Kraven i denna fas baserar sig bland annat på lagstiftning, riskbedömningsresultat, krav (avtal, kunder och intressegrupper) samt verksamhetsomständigheter.

REALISERING - Beslut och planer i den föregående fasen implementeras, kommuniceras och förankras bland såväl personalen som samarbetsparter och kunder.

UPPFÖLJNING – Datasäkerhetsrelaterad teknisk övervakning och rapportering samt bedömning av huruvida de vidtagna åtgärderna har löst de identifierade datasäkerhetsrelaterade problemen och huruvida de har fåtts ner till den planerade nivån. Den tekniska datasäkerheten tillhandahålls av 2M-IT.

FÖRÄNDRINGSHANTERING – Normal förändringshantering inom ramen för förändringshanteringsprocessen utgående från lärdomar som erhållits i samband med uppföljningsfasen.

15. Skyldigheter för anställda och användare

Varje anställd, person som behandlar uppgifter, upprätthåller och använder datasystem eller datanät i Österbottens välfärdsområde är för egen del ansvarig att hörsamma datasäkerhetsprinciperna och ålagd att följa de regler och datasäkerhetsanvisningar som godkänts av välfärdsområdets ledning. Välfärdsområdets anställda har ett övervakningsansvar i frågor som berör datasäkerhet och dataskydd. Användare och upprätthållare ska meddela upptäckta brister i datasäkerhet, missbruk som är förknippade med datasäkerhet eller misstankar om dataskyddsförseelser via HaiPro (datasäkerhetsanmälan) eller genom att kontakta 2M-IT:s Servicedesk. Respektive verksamhetsenhet ansvarar för att givna datasäkerhetsanvisningar följs. Enheternas närchefer och ansvariga användare svarar för att personalen är tillräckligt insatt i de givna anvisningarna och i hur datasystemen ska användas.

16. Datasäkerhetsincidenter

Användningen av data och datasystem övervakas i enlighet med gällande lagar och förordningar med iakttagande av integritetsskyddet i arbetslivet. Samtliga datasäkerhetsincidenter behandlas vederbörligt bland annat på det sätt som beskrivs noggrannare i Österbottens välfärdsområdes anvisning om dataskydd för patientregister.

När en misstanke om en datasäkerhetsincident väcks skickas en begäran om utredning till närchefen som sedan håller ett hörande och upprättar ett protokoll. Beslut i ärendet fattas av den ledande läkaren för ifrågavarande specialitet eller i sista hand av den administrativa överläkaren på basis av den upprättade påföljdstabellen. Ovan nämnda förseelser kan också leda till att en upphävning av anställningsförhållandet inleds. En datasäkerhetsincident kan också leda till straffrättsligt ansvar och att en begäran om utredning tillställs polisen.

17. Centrala begrepp som hänför sig till datasäkerhet

Datasäkerhet

Åtgärder med vilka man strävar efter att trygga riktigheten, integriteten och konfidentialiteten. Datasäkerhet är riskhantering och utgör en del av företagssäkerheten.

Dataskydd

Med dataskydd avses de åtgärder med vilka man skyddar en persons integritet i samband med behandlingen av personuppgifter.

Datasäkerhetspolicy

De mål, principer och realiseringssätt som ledningen godkänt för datasäkerheten.

Datasäkerhetsplanering

En planeringsprocess som inrymmer bland annat en hotanalys, definition av grundtryggheten samt en beredskapsplanering för återhämtning och undantagsförhållanden, vilka utmynnar i datasäkerhetsplaner, linjedragningar och anvisningar.

Datamaterialsäkerhet

Åtgärder som vidtas för att trygga användbarheten, integriteten och konfidentialiteten av handlingar, filer och annat datamaterial bland annat genom att katalogisera och klassificera datamaterial samt genom att hantera, behandla, förvara och förstöra datamedier enligt gällande anvisningar.

Integritet

Åtgärder som används för att bekräfta att information eller meddelande inte har ändrats utan behörighet, men även för att påvisa eventuella förändringar som skett i dokumentationskedjan.

Användbarhet

Åtgärder som är till för att bekräfta att datasystem eller tjänster finns till förfogande och att behöriga aktörer har tillgång till dessa på önskad tid och på fastställt sätt.

Konfidentialitet

Behandling av personuppgifter som gör det möjligt att tillbörligt säkerställa att personuppgifterna är säkra samt skyddade mot obehörig och lagstridig behandling.

18. Delområden som hänför sig till datasäkerhet

Administrativ datasäkerhet

Administrativ datasäkerhet omfattar principer som godkänts av ledningen, ansvarsfördelning, resurser som allokerats för ändamålet samt riskbedömning och tillsyn.

Programsäkerhet

Åtgärder som anknyter till operativsystem och andra program, såsom identifierings-, isolerings, tillgångs- och säkringspraxis, tillsyns- och spårningsåtgärder, loggpraxis och

kvalitetsledning samt åtgärder som anknyter till underhåll och uppdatering av program och som syftar till att främja datasäkerheten.

Datamaterialsäkerhet

Syftet med datamaterialsäkerhet är att bevara konfidentialiteten hos handlingar, poster och filer samt att förhindra att information förstörs eller ändras oavsiktligt. Det är också viktigt att registreringar skyddas och förvaras korrekt. Datamaterialsäkerhet omfattar även åtgärder som vidtas för att information ständigt säkras, förvaras och förstörs på tillbörligt sätt.

Användningssäkerhet

Användningssäkerhet omfattar bl.a. lösenord, kunskaper som möjliggör användning av program som är i bruk samt virusbekämpning. De beviljade användarrättigheterna ska vara anpassade enligt arbetsuppgifterna. Användningssäkerheten består av säkra användningsprinciper, övervakning av informationshantering samt tryggande av kontinuiteten. Driftsäkerheten hos apparaturen utgör också en del av användningssäkerheten. En s.k. återhämtningsplan upprättas för att säkerställa att verksamheten kan fortgå i överraskande lägen.

Utrustningssäkerhet

Åtgärder som anknyter till användbarheten hos utrustning som hänför sig till informationshantering och datatrafik, konfigurering och tillgångsövervakning samt tillgång på reservdelar och tillbehör med vilka man säkerställer att datasäkerheten kan omsättas i praktiken.

Fysisk säkerhet

Skydd av personer, utrustning, material, postförsändelser, lokaliteter och lager mot förstörelse och skador. Fysisk säkerhet omfattar bland annat passage- och lokalitetsövervakning, bevakning, bekämpning av brand-, vatten-, el-, ventilations- och inbrottsskador samt säkerhet som anknyter till kurirer och försändelser av informationsmaterial. Fysisk säkerhet består av många olika delfaktorer, men grunden för säkerheten skapas redan i byggnadsfasen.

Datakommunikationssäkerhet

Genom datakommunikationssäkerhet strävar man efter att säkerställa att de grundläggande målen som uppställts för datasäkerheten, dvs. konfidentialitet, integritet och användbarhet, kan uppnås. Det centrala målet är att säkerställa att meddelandena är ursprungliga, intakta och konfidentiella. Datakommunikationssäkerhet omfattar alla de åtgärder med vilka man kan säkerställa att informationen är skyddad när den rör sig i systemet eller mellan organisationer.

Personalsäkerhet

Målet med personalsäkerhet är att anställda inte på grund av okunnighet, dålig motivation eller illvilja kan ändra eller förstöra information eller kan göra det möjligt för någon utomstående att använda den. Tyngdpunkten i personalsäkerheten ligger på att undvika risker i förväg och på att föregripa att de uppstår.

19. Sammanfattning

Datasäkerheten i välfärdsområdet utvecklas ständigt utgående från datasäkerhetspolicyn och dataskyddspolicyn. Förändringar i systemen skapar en komplex helhet där de som äger

systemen i allt högre grad måste ge akt på datasäkerheten i utvecklings- och produktionsmiljöerna. Även användarnas och anställdas ansvar ökar i takt med att antalet diskreta it-säkerhetsattacker tilltar, vilket innebär att medvetenheten om datasäkerheten också blir viktig. Hela organisationen måste tillsammans utveckla datasäkerheten och samtidigt måste de ändrade befogenheterna i samband med organisationsförändringar tas i beaktande. Dessutom måste också resiliensen och testningen av resiliensen tas i beaktande. Det ofta upprepade talesättet om att datasäkerheten aldrig är fulländad är något som det är viktigt att komma ihåg i 2020-talets komplexa hälso- och sjukvård.

20. Bilagor

Här beskrivs de bifogade bilagor som listats i detta dokument.

1. Datasäkerhetsplan, plats: Version 1.0 Plats: OVPH:s informationsförvaltning
2. Dataskyddspolicy, plats: Version 1.0 Plats: OVPH:s intranät
3. Riskbedömning: Version 1.0 Plats: OVPH:s informationsförvaltning