[Namn på objektet för egenkontroll av informationssäkerheten (organisation)]

Informationssäkerhetsplan

[Datum och uppgifter om eventuella versioner]

[Vem som utarbetat planen]

[Status, eventuella anteckningar om godkännanden och granskningar, datum]

[Eventuell annan information relaterad till dokumentet som behöver synas på förstasidan, till exempel säkerhetsklassificering]

Innehåll

[1. Informationssäkerhetsplanens användningsändamål 3](#_Toc159318439)

[2. Föremålet för informationssäkerhetsplanen och rutiner för uppdatering av planen 4](#_Toc159318440)

[3. Allmänna informationssäkerhetsrutiner 5](#_Toc159318441)

[4. Förfaranden vid fel och problem samt kontinuitetshantering 6](#_Toc159318442)

[5. Personalens utbildning och kompetens samt informationssystemens bruksanvisningar och informationssäker användning av systemen 7](#_Toc159318443)

[5.1 Personalens utbildning samt upprätthållande och utveckling av kompetensen 7](#_Toc159318444)

[5.2 Informationssystemens bruksanvisningar och användning av systemen enligt anvisningarna 8](#_Toc159318445)

[6. Informationssäkerhetsrutiner för informationssystemen 8](#_Toc159318446)

[6.1 Informationssystemens basuppgifter, beskrivningar och uppfyllande av väsentliga krav 8](#_Toc159318447)

[6.1.1 Informationssystem (klass A2 och A3) som ska anslutas till Kanta-tjänsterna 9](#_Toc159318448)

[6.1.2 Andra system för vilka en extern bedömning av informationssäkerheten har gjorts (klass A1) 9](#_Toc159318449)

[6.1.3 Andra system som behandlar kunduppgifter (klass B) 9](#_Toc159318450)

[6.1.4 Andra informationssystem som ska beaktas med tanke på skyddet av känsliga kunduppgifter 9](#_Toc159318451)

[6.1.5 Uppfyllandet av de väsentliga kraven på informationssystem 9](#_Toc159318452)

[6.2 Installation, drift och uppdatering av informationssystemen 10](#_Toc159318453)

[6.3 Rutiner för hantering av behörigheter och identifiering 11](#_Toc159318454)

[6.4 Rutiner för uppföljning av klient- och patientdatasystemens åtkomsthantering och användning 12](#_Toc159318455)

[7. Informationssäkerhetsrutiner för informationssystemens driftmiljö 13](#_Toc159318456)

[7.1 Fysisk säkerhet som en del av säkerheten i informationssystemens driftmiljö 13](#_Toc159318457)

[7.2 Hantering av datorer, mobila enheter och stödtjänster för driftmiljön 13](#_Toc159318458)

[7.3 Informationssäker användning av plattforms- och webbtjänster med tanke på dataskyddet och beredskapen 14](#_Toc159318459)

[8. Informationssäkerhetsrutiner för anslutning till Kanta-tjänsterna och användning av dem 16](#_Toc159318460)

[9. Närmare beskrivningar, anvisningar och planer för varje informationssystem 17](#_Toc159318461)

[9.1 System X (hör till klass A2 och A3) 18](#_Toc159318462)

[9.2 System X (hör till klass A1) 19](#_Toc159318463)

[9.3 System Y (hör till klass B) 20](#_Toc159318464)

[9.4 System Z (övriga system som inte hör till klass A eller B) 20](#_Toc159318465)

# 1. Informationssäkerhetsplanens användningsändamål

[THL:s föreskrift 3/2024 (THL/4/4.05.00/2024) kompletteras med denna **mall för en informationssäkerhetsplan**, dvs. en **dokumentmall som fungerar som exempel** och är avsedd som **stöd för att utarbeta en informationssäkerhetsplan** för objekt för egenkontroll av informationssäkerheten. Dokumentmallens struktur är informativ och vägledande, dvs. den underlättar och styr utarbetandet av planen.

Mallen motsvarar inte till varje detalj, inklusive exempel, THL:s föreskrift 3/2024 – det väsentliga är att vara medveten om att **THL:s föreskrift 3/2024 är förpliktande**; själva mallen kan inte heller direkt vara det, eftersom objekten för egenkontroll av informationssäkerheten är mycket varierande till storlek och typ – organisationer som utför många typer av verksamhet inom social- och hälsovården eller i anslutning till den.]

[Texterna inom **hakparentes** och mindre font (Arial 10) är **kommentarer eller anvisningar till mallen** och kan tas bort från den färdiga informationssäkerhetsplanen eller vid behov lämnas synliga till exempel som underrubriker eller dylikt.

**Mellan anvisningarna** finns på vissa ställen färdiga fraser m.m. med en större font (Arial 11) som underlättar struktureringen av planen. Även dessa ställen kan fritt redigeras enligt behov.]

[Anvisningarna inom hakparentes (från och med kapitel 3 i denna mall för en informationssäkerhetsplan) hänvisar alltid i början av det aktuella kapitlet till motsvarande kapitel i THL:s föreskrift 3/2024. Hänvisningen anges med blå fet stil '**Föreskrift 3/2024**:' och därefter anges det aktuella kapitlets nummer och namn.]

**[Informationssäkerhetsplanen bör ses över och/eller uppdateras regelbundet**. Ansvaret för att utarbeta och följa informationssäkerhetsplanen ligger hos den ansvariga föreståndaren hos en tjänstetillhandahållare inom social- och hälsovården och en apotekare enligt 78 § i lagen om kunduppgifter.]

[Det är frivilligt att använda mallen för informationssäkerhetsplanen. **Objekten för egenkontroll av informationssäkerheten kan utarbeta informationssäkerhetsplanen på det sätt som de anser ändamålsenligt**, förutsatt att den information som presenteras i THL:s föreskrift 3/2024 tydligt framgår av planen och dess eventuella bilagor (dokument som informationssäkerhetsplanen hänvisar till). Informationssäkerhetsplanen är ett praktiskt verktyg för att upprätthålla och utveckla den övergripande säkerheten.]

[**I informationssäkerhetsplanen kan man använda sig av** all befintlig dokumentation i organisationen och **hänvisa till denna i planen**. Informationssäkerhetsplanen kan alltså vara en **plan som sammanställer** andra planer och anvisningar.]

[**Endast denna version av mallen har upprättats som bilaga till THL:s föreskrift 3/2024**. Tjänstetillhandahållare inom social- och hälsovården som till sin storlek och verksamhet är mycket annorlunda kan tillämpa eller komplettera mallen genom att spegla sin egen verksamhet. Det väsentliga är att skyldigheterna enligt 77 § 1 och 2 mom. i lagen om kunduppgifter 703/2023 uppfylls.[[1]](#footnote-1)]

När informationssäkerhetsplanen uppdateras är det bra att börja med de områden som är mest kritiska med tanke på **informationssäkerhetsstatusen och de risker som identifierats i den egna verksamheten** hos objektet för egenkontroll av informationssäkerheten.]

[När man utarbetar informationssäkerhetsplanen kan man använda till exempel följande källor:

* Traficoms Cybersäkerhetscenters cybermätare – ett verktyg för att bedöma och utveckla cybersäkerheten i organisationer: [https://www.kybermittari.fi/](https://www.kyberturvallisuuskeskus.fi/sv/vara-tjanster/lagesbild-och-natverksledarskap/cybermataren)
* Kriterier för bedömning av informationssäkerheten i den offentliga förvaltningen (Julkri), Rekommendation och kriterier (6/2023): <https://julkaisut.valtioneuvosto.fi/handle/10024/165016>
* Dataombudsmannens byrå – Överföring av personuppgifter till länder utanför Europeiska ekonomiska samarbetsområdet:
<https://tietosuoja.fi/sv/overforing-av-personuppgifter-till-lander-utanfor-ees>
* Cybersäkerhetscentret – Krav på informationssäkerhet och dataskydd vid upphandling inom social- och hälsovården: <https://www.kyberturvallisuuskeskus.fi/sv/aktuellt/anvisningar-och-guider/krav-pa-informationssakerhet-och-dataskydd-vid-upphandling-inom>]
* Myndigheten för digitalisering och befolkningsdata 12/2022 – Referensram för arkitekturen för digital säkerhet (på finska): <https://wiki.dvv.fi/display/DTARK/>]

Detta dokument utgör informationssäkerhetsplanen för [organisationens namn]. Syftet med denna informationssäkerhetsplan är att uppfylla skyldigheterna enligt 77 § 1 och 2 mom. i lagen om kunduppgifter[[2]](#footnote-2) 703/2023 och THL:s föreskrift 3/2024. Planen sammanställer de redogörelser och krav som krävs av tjänstetillhandahållare, apotek, mellanhänder och Folkpensionsanstalten.

# 2. Föremålet för informationssäkerhetsplanen och rutiner för uppdatering av planen

Denna informationssäkerhetsplan omfattar:

[I kapitel 2 i informationssäkerhetsplanen redogörs för den aktör eller de aktörer, objektet för egenkontroll av informationssäkerheten, som just denna informationssäkerhetsplan gäller:

* en eller flera tjänstetillhandahållare
* apotek
* mellanhänder
* FPA.

Jfr följande kapitel i THL:s föreskrift 3/2024: 1 Föreskriftens syfte och tillämpningsområde, 2 Definitioner och 3 Ansvar för säkerställande av informationssäkerheten och ändamålsenlig behandling av kunduppgifter

[Här anges grundläggande uppgifter om den/de aktörer som är föremål för informationssäkerhetsplanen]

* Namn: [tjänstetillhandahållarens/verksamhetsenhetens namn]
* FO-nummer: [FO-nummer]
* Ansvarig person/chef: [namn på tjänstetillhandahållarens/verksamhetsenhetens chef]
* Verksamhetsställen/serviceenheter: [alla serviceenheter och/eller verksamhetsställen som berörs av planen]
* Underleverantörer och avtalsparter som omfattas av planen: [tjänstetillhandahållare som är verksamma inom ramen för den här planen (till exempel genom uppdrags- eller underleverantörsavtal) och som berörs av planen]
* …

Vid genomförandet och uppdateringen av planen iakttas följande rutiner:

* Person som ansvarar för planen och uppdateringen av den: [namn]
* Personer som ansvarar för genomförandet av planen: [personer som ansvarar för dataskydds- och informationssäkerhetsåtgärder i praktiken]
* Praxis för granskning och uppdatering: [beskrivning av praktiska åtgärder och metoder med vilka planen tas i bruk och beskrivning av hur ofta planen granskas (ses över) och vid behov uppdateras regelbundet, även i vilka situationer planen granskas och uppdateras]
* Uppföljning av planen och dokumentation av uppföljningen: [Beskrivning av på vilket sätt genomförandet av planen regelbundet följs upp och hur uppföljningen dokumenteras. Roller för eventuella informationssäkerhetsgrupper eller motsvarande]
* Användning av planen vid upphandling och uppdatering av informationssystem: [beskrivning av hur de åtgärder som beskrivs i planen beaktas då man upphandlar eller uppdaterar informationssystem]
* Beslut om godkännande och ibruktagande av planen: [vem/vilka/vilken aktör som beslutat att godkänna och ta i bruk planen och när beslutet fattats, hur man beslutar om att godkänna och ta i bruk nya versioner av planen]
* …

# 3. Allmänna informationssäkerhetsrutiner

[**Föreskrift 3/2024**: 6.1 Allmänna informationssäkerhetsrutiner]

[I detta kapitel anges information om allmänna informationssäkerhetsrutiner, policyer i anslutning till digital säkerhet, ansvarsfördelning och organisering av informationssäkerhetsarbetet (kan beskrivas i policyerna), register över behandling av personuppgifter, avtal, centrala informationssäkerhetsanvisningar samt dataskyddsombud]

[Organisationens namn] iakttar följande allmänna informationssäkerhetsrutiner och utför arbete med informationssäkerhet, dataskydd, riskhantering och egenkontroll av behandlingen av kunduppgifter enligt följande dokument:

Informationssäkerhetsarbetet utförs enligt följande dokument:

[Hänvisningar till dokument som organisationen använder för att säkerställa och utveckla dataskyddet och informationssäkerheten, till exempel:

* informationssäkerhetspolicy, dataskyddspolicy, policy för digital säkerhet eller motsvarande dokument
* riskhanteringspolicy och planer för underhåll och utveckling av riskhanteringen
* register över behandlingen av personuppgifter[[3]](#footnote-3)
* förteckning över avtalsparter med underleverantörer i anslutning till behandling av uppgifter och informationssäkerhet som omfattas av informationssäkerhetsplanen: stödtjänster för driftmiljön, informationssystemtjänster och andra eventuella tjänster
* informationssäkerhetsanvisningar för producenter av informationssystemtjänster
* egna informationssäkerhetsanvisningar
* anvisningar om informationssäkerhet vid distans- och hybridarbete
* förteckning över övriga anvisningar och beskrivningar som ska iakttas
* eventuell kvalitetshandbok
* …]

Dataskyddsombud: [Här anges dataskyddsombudets/dataskyddsombudens namn]

# 4. Förfaranden vid fel och problem samt kontinuitetshantering

[**Föreskrift 3/2024**: 6.2 Förfaranden vid fel och problem samt kontinuitetshantering]

[För utarbetandet av informationssäkerhetsplanen kan man i detta kapitel använda sig av

* eOppivas material som är öppet för alla (publicerat 2020): <https://www.eoppiva.fi/koulutukset/trygga-den-digitala-verksamheten-vid-storningar/>
* Myndigheten för digitalisering och befolkningsdata, verktyg för klassificering av kritiska objekt: <https://dvv.fi/sv/publikationer-om-digital-sakerhet> (Publikationer från 2022 / Verktyg och modeller)
* Anvisning, framtagen inom projektet Kyber-Terveys, för klassificering av kritiskheten hos funktioner och informationssystem inom en social- och hälsovårdsorganisation (publicerad 2022): <https://www.kyberturvallisuuskeskus.fi/sv/aktuellt/anvisningar-och-guider/klassificering-av-kritiskheten-hos-funktioner-och>]

I beredskapen inför exceptionella situationer och planeringen av kontinuiteten iakttas följande tillvägagångssätt:

[Hur kontinuitetsplaneringen och beredskapen ordnas, till exempel:

* olika planer som hör till temat (kontinuitet, återhämtning, beredskap)
* praktisk övning, beredskapsverksamhet, anvisningar, tillgång till anvisningar
* eventuella upphandlingar relaterade till återhämtning från störningar i informationssystemen
* förhållanden som avviker från det normala, kortvariga och långvariga störningar, exceptionella förhållanden
* beredskap för verksamhet i exceptionella situationer utan informationssystem och/eller plattforms- och webbtjänster
* klassificeringarna av hur kritiska informationssystemen är och deras eventuella inverkan på beredskapsrutinerna
* …]

Vid fel och problem samt återhämtning från dem iakttas följande tillvägagångssätt:

[Beskrivning av hur man går till väga för att utreda fel och problem och återhämta sig från dem, ansvaren vid fel och exceptionella situationer, vid behov olika fel och problem var för sig, till exempel:

* problem med nätet eller telekommunikationerna (förfaranden och kontaktuppgifter till producenter av nättjänster, eventuella anvisningar av producenterna)
* problem med användningen av informationssystemen (förfaranden om systemet inte fungerar, inte startar eller fungerar felaktigt, olika systemleverantörers kontaktuppgifter och stödtjänster)
* praxis för genomförande av beredskap till följd av klassificeringarna av hur kritiska informationssystemen är
* åtgärder för att hantera informationssystem, deras delsystem och komponenter
- åtgärder för övervakning, drift och uppdatering
-...
* hantering av misstänkta, observerade eller realiserade informationssäkerhets- eller dataskyddshot eller problem
- åtgärder om klient- eller patientuppgifter eller andra uppgifter som ska skyddas har läckt ut till utomstående
- åtgärder om virusprogram eller skadliga program upptäcks
- åtgärder om en anställds användaruppgifter har läckt ut till utomstående
- åtgärder om nätfiske upptäcks

Väsentliga uppgifter om dataskyddsavvikelser och redogörelse för de bakomliggande orsakerna

* möjliga rapporteringskanaler för anmälan av dataskyddsavvikelser
* åtgärder om informationssystem som behandlar klient- eller patientuppgifter tydligt fungerar på fel sätt i förhållande till de nationella krav som ställs på dem, hur producenten av en informationssystemtjänst eller tillsynsmyndigheterna underrättas om saken
- det vill säga anmälan till producenten av en informationssystemtjänst om betydande avvikelser som iakttagits i fråga om uppfyllandet av väsentliga krav på system i klass A eller klass B
* åtgärder om ett informationssystem som behandlar klient- eller patientuppgifter medför en risk för klient- och/eller patientsäkerheten
- det vill säga anmälan till Valvira om betydande avvikelser i system som hör till klass A eller klass B, om avvikelserna medför en betydande risk för klient- och/eller patientsäkerheten eller informationssäkerheten
- till exempel i situationer där klient- och/eller patientuppgifter och/eller receptuppgifter har gått till fel kund/patient på grund av ett systemfel
* åtgärder vid dataskyddsavvikelser, anmälan till dataombudsmannen och de registrerade
* åtgärder vid tillbud i anslutning till medicintekniska produkter, om informationssystemet eller välbefinnandeapplikationen uppfyller definitionen av en medicinteknisk produkt, anmälan till Fimea
* åtgärder i återhämtningsskedet/-skedena samt fortsatta utvecklingsåtgärder utifrån erhållna erfarenheter efter att verksamheten återgått till normalläget -> kontinuerlig utveckling av kontinuitetshanteringen
* …]

# 5. Personalens utbildning och kompetens samt informationssystemens bruksanvisningar och informationssäker användning av systemen

## 5.1 Personalens utbildning samt upprätthållande och utveckling av kompetensen

[**Föreskrift 3/2024**: 6.3 Personalens utbildning samt upprätthållande och utveckling av kompetensen]

[Eventuella hänvisningar till separata planer för uppföljning av utbildning och/eller kompetens]

[Hur man säkerställer att personalen har fått utbildning i användning av informationssystem, behandling av klient- och patientuppgifter samt dataskydds- och informationssäkerhetsfrågor. Dessutom ska man beskriva hur personalens kompetens följs upp och upprätthålls.]

Behandlingen av klient- och patientuppgifter, användningen av informationssystem samt genomförandet av dataskydd och informationssäkerhet i utbildningar, anvisningar och uppföljning sker på följande sätt:

[Beskrivning av till exempel

* hur man säkerställer att personalen har fått utbildning och introduktion i verksamhetsmodeller och arbetssätt gällande behandling av klient- och patientuppgifter (till exempel hur de informerar klienter och patienter, besvarar begäran om information osv.)
* hur man ombesörjer utbildning och introduktion i användningen av informationssystemen och nya versioner av dem samt regelbundet upprätthållande av kompetensen i olika arbetsuppgifter och roller
* hur man genomför utbildning i dataskydd och informationssäkerhet och vid behov hänvisningar till separata utbildningsplaner
* hur man följer upp fullföljandet av utbildningar och inlärningen (till exempel intyg eller uppgifter som ska upprätthållas om deltagande i utbildningar)
* vem som ansvarar för kostnaderna för olika utbildningar, vid behov hänvisningar till relevanta avtal
* …]

## 5.2 Informationssystemens bruksanvisningar och användning av systemen enligt anvisningarna

[**Föreskrift 3/2024**: 6.4 Informationssystemens bruksanvisningar och användning av systemen enligt anvisningarna]

Följande tillvägagångssätt iakttas för hantering av och tillgång till informationssystemens bruksanvisningar och för användning av systemen enligt anvisningarna:

[Beskrivningar av till exempel

* hur man har säkerställt att informationssystemets användare har tillgång till nödvändiga bruksanvisningar i begriplig skriftlig form (inklusive alla nödvändiga språkversioner) – vid behov både organisations- och informationssystemspecifika anvisningar
* hur anvisningarna om behandlingen av klient- och patientuppgifter har dokumenterats och kan verifieras
* hur man genom dokumentation bevisar att personalen deltar i utbildningar om behandling av klient- och patientuppgifter
* hur upprätthållandet av personalens kunskaper har ordnats
* hur uppdatering och distribution av bruksanvisningar sker i samband med versionsuppdateringar av programvara och andra ändringar (verksamhetsmodeller)
* hur man stöder (introduktion, handledning, rådgivning) anställda med olika arbetsuppgifter och roller i användningen av system som behandlar klient- eller patientuppgifter
* …]

# 6. Informationssäkerhetsrutiner för informationssystemen

## 6.1 Informationssystemens basuppgifter, beskrivningar och uppfyllande av väsentliga krav

[**Föreskrift 3/2024**: 6.5 Informationssystemens basuppgifter, beskrivningar och uppfyllande av väsentliga krav]

Beskrivningar av de informationssystem och välbefinnandeapplikationer som används och vilka rutiner som iakttas vid genomförandet och uppföljningen av behandlingen av kunduppgifter, dataskyddet och informationssäkerheten vid användningen av dessa informationssystem:

**[Det är ofta lämpligt att börja med att sammanställa innehållet i den här punkten]**

[Beskrivningar av informationssystemen: Jfr kapitel 9 i mallen (inkl. närmare beskrivningar)]

Informationssystemspecifika beskrivningar, anvisningar och planer De informationssystem som används ska beskrivas och klassificeras utifrån hur kritiska de är. Obs! Praxis för genomförande av beredskap till följd av klassificeringarna av hur kritiska informationssystemen är beskrivs i kapitel 4 i mallen]

[Till exempel hänvisningar till en separat aktuell förteckning över informationssystem eller en informationssystemsportfölj som ska underhållas, eller en förteckning över de system som används. Görs vid behov i samarbete med leverantören av informationssystemet eller informationssystemlösningen]

[Alla system som påverkar behandlingen av klientuppgifter inom socialvården eller patientuppgifter, informationssäkerheten och dataskyddet inkluderas]

[Förutom beskrivningar av informationssystemen ska informationssäkerhetsplanen också innehålla beskrivningar av **välbefinnandeapplikationer** och andra **digitala ärendetjänster** som riktas till kunder och som används i verksamheten av objektet för egenkontroll av informationssäkerheten. (I THL:s föreskrift 4/2024, kapitel 2 Definitioner, definieras välbefinnandeapplikationer och digitala ärendetjänster som tillsammans bildar en **digital tjänst**.)[[4]](#footnote-4)]

### 6.1.1 Informationssystem (klass A2 och A3) som ska anslutas till Kanta-tjänsterna

[Förteckning över basuppgifterna för varje **system och välbefinnandeapplikation**: namn, version (eller motsvarande statusinformation), leverantör, kontaktuppgifter, uppgifter om FPA:s samtestning, uppgifter om intyget över bedömning av informationssäkerheten och hur detta motsvarar uppgifterna i Valviras register över informationssystem] Även uppgifter om digitala ärendetjänster i anslutning till den egna verksamheten]

### 6.1.2 Andra system för vilka en extern bedömning av informationssäkerheten har gjorts (klass A1)

[Förteckning över basuppgifterna för varje **system och välbefinnandeapplikation**: namn, version (eller motsvarande statusinformation), leverantör, kontaktuppgifter, uppgifter om intyget över bedömning av informationssäkerheten och hur detta motsvarar uppgifterna i Valviras register över informationssystem] Även uppgifter om digitala ärendetjänster i anslutning till den egna verksamheten]

### 6.1.3 Andra system som behandlar kunduppgifter (klass B)

[Förteckning över basuppgifterna för varje **system**: namn, version (eller motsvarande statusinformation), leverantör, kontaktuppgifter och hur dessa motsvarar uppgifterna i Valviras register över informationssystem Även uppgifter om digitala ärendetjänster i anslutning till den egna verksamheten]

### 6.1.4 Andra informationssystem som ska beaktas med tanke på skyddet av känsliga kunduppgifter

[Förteckning över basuppgifterna för varje system: namn, version (eller motsvarande statusinformation), leverantör och kontaktuppgifter. Även uppgifter om digitala ärendetjänster i anslutning till den egna verksamheten]

### 6.1.5 Uppfyllandet av de väsentliga kraven på informationssystem

[Beskriv vilka åtgärder objektet för egenkontroll av informationssäkerheten har vidtagit för att säkerställa att de väsentliga kraven på informationssystemen och välbefinnandeapplikationerna uppfylls, bland annat:

* upphandlingar, avtal och som en del av dem säkerheter om att informationssystemen och välbefinnandeapplikationerna uppfyller de minimikravprofiler som behövs i verksamheten
* granskning av giltigheten för uppgifterna och överensstämmelsen med kraven i Valviras register över informationssystem för de informationssystem och välbefinnandeapplikationer som används eller uppdateras
* förfaranden för uppdatering av uppgifter
* säkerställande av informationssystemens prestanda i olika situationer utan att informationssäkerhets- och dataskyddsegenskaperna äventyras
* …]

## 6.2 Installation, drift och uppdatering av informationssystemen

[**Föreskrift 3/2024**: 6.6 Installation, drift och uppdatering av informationssystemen]

Vid installation, drift och uppdatering av informationssystemen iakttas följande tillvägagångssätt:

[I kapitel 6.1 och 9 i mallen kan man beskriva systemspecifika rutiner, om flera system används och de avviker från rutinerna som anges här]

[Beskrivning av rollerna för installation, drift och uppdatering av systemen, förfaranden för ändringshantering, testning och godkännande samt ansvar i allmänhet och åtgärder för att säkerställa informationssäkerheten för åtminstone följande:

* säkerställande i Valviras register över informationssystem av att ett informationssystem får användas för produktion av tjänster
* vilka personer och aktörer som får utföra installationsåtgärder i systemen
* hur man förhindrar att andra personer kan utföra installationer i system eller programvara, till exempel om det krävs informationssäkerhetsutredningar eller säkerhetsutredningar av personer som arbetar med vissa uppgifter eller tjänster eller av tjänsteproducenter
* yrkeskunskaper eller utbildning som krävs av personer som utför installations-, drift- och uppdateringsåtgärder
* vilka tjänster och applikationer som finns i informationssystemen eller deras delsystem
* vilka roller och ansvar personerna som installerar, driver och uppdaterar informationssystemen har i förhållande till objektet för egenkontroll av informationssäkerheten och producenten av en informationssystemtjänst
* hur man förhindrar att informationssystem eller programvara innehåller aktiva standardanvändaruppgifter eller andra eventuella standardinställningar som utgör en risk för informationssäkerheten (hänvisningar exempelvis till härdningsanvisningar)
* hur informationssystemen skyddas mot de vanligaste informationssäkerhetsbristerna och sårbarheterna i webbapplikationer
* tillvägagångssätt om det system som används uppdateras
* vad som åtminstone måste testas och säkerställas innan ett system eller en ny systemversion tas i användning för produktion av tjänster
* hur man godkänner ibruktagandet av ett nytt system eller en ny systemversion, ansvar för godkännande
* vid behov hänvisningar eller mallar till avtal eller andra dokument (till exempel avseende testning och ändringshantering) där dessa omständigheter beskrivs
* förfaranden för underhåll, förnyelse, drift och uppdatering av de viktigaste och mest kritiska informationssystemen för social- och hälsovården samt av de fysiska delarna och programvaran i de enheter som behövs i informationssystemens verksamhet samt av enskilda komponenter i anslutning till dessa
* hur man säkerställer tillförlitligheten hos de mest kritiska informationssystemen för social- och hälsovården (bland annat dupliceringar, tillfälliga lösningar, reservdelar och specialkomponenter) genom aktiva övervaknings- och underhållsåtgärder]
* …]

## 6.3 Rutiner för hantering av behörigheter och identifiering

[**Föreskrift 3/2024**: 6.7 Rutiner för hantering av behörigheter och identifiering]

[I kapitel 6.1 och 9 i mallen kan man beskriva systemspecifika rutiner, om flera system används och de avviker från rutinerna som anges här]

[Vid behov hänvisningar till separata interna eller externa anvisningar eller beskrivningar]

De personer och grupper som använder informationssystemen och enheterna administreras på följande sätt:

[Beskrivningar av åtminstone följande:

* hur och var man upprätthåller en aktuell förteckning över de användare och vid behov användargrupper som använder socialvårdens klient- och/eller patientdatasystem
* hur och var man upprätthåller en aktuell förteckning över de användare och vid behov användargrupper som använder företagets enheter (datorer, mobila enheter, andra enheter)
* hur och var man upprätthåller en aktuell förteckning över åtkomsträttigheter till Kanta-tjänsterna
* hur och var man upprätthåller en aktuell förteckning över åtkomsträttigheter till andra elektroniska system
* …]

I fråga om uppföljning av åtkomsträttigheter och behörigheter iakttas följande tillvägagångssätt:

[Beskrivningar av åtminstone följande:

* olika roller i anslutning till hanteringen av behörigheter och personer som innehar de olika rollerna (ansökan om samt beviljande, ändring, återkallelse och fråntagande av behörigheter)
* förfaranden för hantering av behörigheter (eventuella IAM-system som används)
* rutiner för ansökan om samt beviljande, uppföljning, ändring, översyn/säkerställande och fråntagande av behörigheter, till exempel:
	+ hur en ny anställd eller vikarie (i olika praktiska situationer och vid olika klockslag) får användaruppgifter och åtkomsträttigheter
	+ hur vikariernas identitet verifieras innan de beviljas åtkomsträttigheter
	+ hur och när en före detta anställd fråntas sina användaruppgifter och åtkomsträttigheter
	+ vem/vilka som har rätt att godkänna åtkomsträttigheter
	+ …
* praktiska åtgärder i brådskande situationer där åtkomsträttigheter eller användaruppgifter måste fråntas
* hantering av åtkomsträttigheter vid användning av Kanta-tjänsterna
* …]

Vid identifiering och verifiering av användare iakttas följande rutiner:

[Beskrivningar av åtminstone följande:

* praxis för hantering av yrkeskort och lösenord samt andra inloggnings- och identifieringsverktyg (separat plan); åtminstone för passerkontroll, inloggning på datorer och i system samt inloggnings- och identifieringsrutiner för mobila enheter
* användningen av annan stark elektronisk autentisering
* användningen av identifiering med användarnamn och lösenord
* användningen av gemensamma användarnamn i avgränsade och nödvändiga objekt (icke-identifierande) och hur användningen av dem i andra objekt förhindras
* eventuell användning av multifaktorautentisering (MFA)
* administratörers och informationssystemexperternas verksamhet och identifiering vid felutredningar
* eventuellt utnyttjande av datatekniska säkerhetsrutiner för passerkontroll (anknyter till punkt 7.1 i mallen)
* …]

## 6.4 Rutiner för uppföljning av klient- och patientdatasystemens åtkomsthantering och användning

[**Föreskrift 3/2024**: 6.8 Rutiner för uppföljning av åtkomsthantering och användning av klient- och patientdatasystem]

[Vid behov hänvisningar till separata interna eller externa anvisningar/beskrivningar]

Åtkomsthantering och uppföljning av användningen av system som behandlar kunduppgifter genomförs på följande sätt:

[I planen för uppföljning och övervakning av dataskyddet och behandlingen av kunduppgifter beskrivs åtminstone följande:

* vilka kontroller av åtkomsthanteringen som görs vid inloggning i enheter, när informationssystemen startas och eventuellt i andra situationer, såsom vid passerkontroll
* tekniska förfaranden för åtkomsthantering för att förhindra otillåten användning i informationssystem som behandlar klientuppgifter inom socialvården eller patientuppgifter samt de egna anvisningar och tillvägagångssätt som objektet för egenkontroll av informationssäkerheten tillämpar för korrekta arbetssätt och korrekt behandling av uppgifter
* förteckningar eller motsvarande sammanställningar av loggar från informationssystemen för att följa upp användningen av klientuppgifter inom socialvården och patientuppgifter (bland annat loggfiler, logghanteringssystem etc.)
* rutiner för uppföljning av logghantering och användning vid övervakning och när man svarar på begäran om information
- centrala roller, bland annat rollerna för dataskyddsombudet, informationsförvaltningen och de som ansvarar för registerföringen i uppföljningen av användningen av kunduppgifter
- de logghanteringssystem och/eller andra rapporteringsmetoder som används
- hur kundernas begäran om information besvaras, vem/vilka som sammanställer loggrapporterna och hur ofta
- vem/vilka som följer upp loggrapporterna eller logguppgifterna och hur ofta
* verksamhetsmodell när lagstridig behandling av klientuppgifter inom socialvården eller patientuppgifter misstänks eller upptäcks
- beskrivning av tillvägagångssätten för intern kontroll vid eventuella misstankar om förseelser
- beskrivning av hur man går till väga om fel eller misstankar om förseelser eller obehörig användning avslöjas i logguppgifterna
* tillgång till och anskaffning av FPA:s logguppgifter för uppföljning och övervakning. FPA kan lämna ut uppgifter ur utlämningsloggregistret till registrets personuppgiftsansvarige och receptcentrets logguppgifter till tjänstetillhandahållare eller apotek i uppföljnings- och övervakningssyfte
– beskrivning av verksamhetsmodell och praktiska förfaranden
* eventuella andra uppföljnings- och rapporteringsförfaranden, till exempel utnyttjande av databokslut för att uppfylla den personuppgiftsansvariges ansvarsskyldighet
* …]

# 7. Informationssäkerhetsrutiner för informationssystemens driftmiljö

## 7.1 Fysisk säkerhet som en del av säkerheten i informationssystemens driftmiljö

[**Föreskrift 3/2024**: 6.9 Fysisk säkerhet som en del av säkerheten i informationssystemens driftmiljö]

Den fysiska säkerheten tryggas i driftmiljön för kunduppgifter och informationssystem som en del av säkerställandet av informationssäkerheten på följande sätt:

[Beskrivningar av åtminstone följande:

* hur man ser till att lokalerna är låsta för obehöriga, hur passerkontrollen ordnas osv.
* placering av bildskärmsterminaler och rutiner för att skydda dem så att obehöriga inte kan se uppgifter på dem, till exempel placering av terminaler, sekretessfilter, låstid och lösenord för oanvända terminaler
* hur och inom vilka tidsgränser man fastställer att en session ska avbrytas eller tidsgränsen för låsning av användargränssnittet i system där man måste låsa användargränssnittet eller förhindra att det används
* rutiner för distans- och hybridarbete i olika mobila patient- och klientarbeten
* vem som har rätt att installera program och applikationer på organisationens enheter, hur man ser till att endast dessa personer kan utföra installationer
* huruvida användning av externa hårddiskar och usb-minnen tillåts och skyddsrutinerna kring dessa, till exempel endast lagringsmedier som företaget själv har skaffat tillåts, skydd med lösenord, hur man förhindrar att obehöriga inte kan använda lagringsverktyg på datorer eller det interna nätverket (gäller bland annat skydd mot skadliga program)?
* var skrivare har placerats och hur man förhindrar obehöriga från att komma åt skrivarna, eventuella lösningar för säkerhetsutskrifter
* hur man i anslutning till arkivfunktionen förvarar pappersutskrifter som innehåller klientuppgifter inom socialvården eller patientuppgifter inlåsta i ett brandsäkert utrymme och skyddade från obehöriga samt hur de förstörs så att obehöriga inte kommer åt uppgifterna
* praktiska lösningar för förstöring av pappersutskrifter, till exempel låsbara behållare och dokumentförstörare, vilket ansvar personer som gör utskrifter och använder utskrifter har för utskrifternas säkerhet
* eventuellt utnyttjande av datatekniska säkerhetsrutiner för passerkontroll (anknyter till punkt 6.4 i mallen)
* …]

## 7.2 Hantering av datorer, mobila enheter och stödtjänster för driftmiljön

[**Föreskrift 3/2024**: 6.10 Hantering av datorer, mobila enheter och stödtjänster för driftmiljön]

Informationssäkerheten för datorer, mobila enheter och stödtjänster för driftmiljön tillgodoses på följande sätt:

[Beskrivningar av åtminstone följande:

Datorer och mobila enheter,

* hur man i praktiken har säkerställt att datorernas virusskydd fungerar och uppdateras
* hur rutiner för att skydda mobila enheter (datorplattor och smarttelefoner, eventuella bärbara datorer) har ordnats, till exempel användarnamn, lösenord, pinkoder, hantering av sim-kort och enheternas antivirusprogram, fjärrlåsning och/eller tömning av borttappade mobila enheter
* praxis för radering av uppgifter från enheter när anställningsförhållanden upphör
* …

Stödtjänster för driftmiljön,

* Hur man ordnar allmänna stödtjänster för driftmiljön: till exempel uppdateringar av operativsystemet och systemprogram, såsom MS Office, eventuella härdningar, säkerställande av interoperabiliteten och uppföljning av situationen med social- och hälsovårdssystemen
* …

Beskrivning av driftmiljön i anslutning till frågor om ansvars- och arbetsfördelning mellan egen och utlagd verksamhet,

* olika roller och rutiner i driftmiljön
* avtalsparter och deras eventuella underleverantörer
* …]

## 7.3 Informationssäker användning av plattforms- och webbtjänster med tanke på dataskyddet och beredskapen

[**Föreskrift 3/2024**: 6.11 Informationssäker användning av plattforms- och webbtjänster med tanke på dataskyddet och beredskapen]

Plattforms- och webbtjänsternas informationssäkerhet tillgodoses på följande sätt:

[**Jfr underpunkterna a–j till kapitel 6.11 i föreskrift 3/2024**]

[Beskrivningar till exempel av följande (om sådana tjänster används av objektet för egenkontroll av informationssäkerheten):

Allmänt,

* Förteckningar över de plattforms- och webbtjänster som används samt ansvaret för hanteringen av dem: tjänstetillhandahållare, producenter av informationssystemtjänster, tredje parter (underleverantörer)
* Påvisande av att dataskyddsbestämmelserna är lagenliga i den egna verksamheten när externa tjänsteproducenters plattforms- och webbtjänster används (till exempel eventuella hänvisningar till avtal och informationssäkerhetsrutiner)
* Beredskap för verksamhet i exceptionella situationer utan centrala informationssystem (jfr kapitel 4 i mallen. Förfaranden vid fel och problem samt kontinuitetshantering) – planering av IT- och icke-IT-metoder och informationshantering.

Servrar och servermiljöer,

* vilka tjänster och applikationer som finns på servrarna och vem som ansvarar för deras installation och drift
* hur de servrar som informationssystemen använder skyddas mot skadliga program och rutinerna för hur man uppdaterar de program som bekämpar skadliga program
* hur man förhindrar att servermiljön inte innehåller aktiva standardanvändaruppgifter eller andra standardinställningar som utgör en risk för informationssäkerheten
* hur installationen av servrarnas informationssäkerhetsuppdateringar har beskrivits och ordnats, hur man bedömer behovet av uppdateringarna och hur kritiska de är, hur uppdateringarna testas och godkänns i en separat testmiljö innan de installeras i produktionsmiljön
* …

Hantering av datanät, nätverksenheter, trådlösa nätverk och routrar,

* hur har man kommit överens om ansvaret för datakommunikationsoperatörerna och informationssäkerheten inom datakommunikationen, huruvida avtalen innehåller frågor om informationssäkerhet och tjänstens tillgänglighet, inklusive kontakter och förfaranden vid störningar
* hur man har ordnat informationssäkerhetsrutiner för de nätverk som används (till exempel segmenteringar, brandväggar, dirigering)
* krav på lösenord i trådlösa nätverk, rutiner för byte av lösenord, skydd av företagets eget trådlösa nätverk mot obehöriga användare
* om kunderna erbjuds ett trådlöst nätverk, hur det separeras från organisationens eget nätverk
* ansvar för uppdateringar och skydd av routrar och andra nätverksenheter och eventuella avtal i anslutning till dessa
* uppdateringar av komponenter samt programvara i routrar och andra nätverksenheter
* …

Fjärranslutningar och deras informationssäkerhet – här kan man hänvisa till organisationens eventuella anvisningar för distansarbete där motsvarande frågor som gäller informationssäkerhet och dataskydd har behandlats,

* vilka tjänster eller system som får användas på distans, hur man förhindrar/förbjuder distansanvändning av andra tjänster
* vilka eller vilken typ av internettjänster får och får inte användas på datorerna
* med vilken typ av anslutningar och informationssäkerhetslösningar kan och får tjänster användas på distans (till exempel VPN-anslutning)
* anslutningar och rutiner för underhåll av utrustning och programvara
* anvisningar till anställda och andra användare om dataskydd och informationssäkerhet i samband med fjärråtkomst
* …

Molntjänster, molnbaserade lösningar, fjärradministrationstjänster, serveruthyrning, serverhantering, backuptjänster och datorhallstjänster,

* bedömning av riskerna i samband med behandling av personuppgifter (konsekvensbedömning enligt EU:s allmänna dataskyddsförordning) i alla verksamheter och eventuella underleverantörskedjor i anslutning till dem
* beskrivningar av bedömningen av risknivån vid överföring av personuppgifter till tredjeländer med tillhörande granskningar av nödvändiga organisatoriska, avtalsbaserade och tekniska skyddsåtgärder från fall till fall och i varje land
* beskrivningar av alla molntjänster som används (de olika typerna av molntjänster och skillnaderna mellan dessa) i anslutning till de informationssystem som används; även hänvisningar till avtal i anslutning till dessa
* hur avtalens aktualitet motsvarar gällande bestämmelser (bland annat EU:s allmänna dataskyddsförordning, vid behov grunderna för överföring av personuppgifter utanför EES-området)
* beskrivningar av den kontinuerliga och regelbundna uppföljningen av de plattforms- och webbtjänster (inklusive molntjänster) som används, bland annat med tanke på funktionaliteten, informationssäkerhetsriskerna, störningar och användarvillkoren för tjänsterna (uppdatering av avtal och rutiner så att de motsvarar den förändrade situationen)
* planen för drift, uppdatering och förnyelse av informationssystem, delsystem, komponenter och nätverk samt en verksamhetsmodell för beslutsfattande om underhållsåtgärder
beredskapsperspektivet när informationen också behöver finnas tillgänglig under förhållanden som avviker från det normala; planen ska bland annat beskriva hur informationshanteringen ordnas i en eventuell situation där samhällets nätförbindelser är begränsade till Finlands geografiska gränser.]

[Vid behov kan man utnyttja bland annat följande källor:

* Dataombudsmannens byrå, Överföring av personuppgifter till länder utanför Europeiska ekonomiska samarbetsområdet:
<https://tietosuoja.fi/sv/overforing-av-personuppgifter-till-lander-utanfor-ees>
* Säkerhetskriterierna för molntjänster (PiTuKri):
<https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/file/Traficom_PiTuKri_2020_SE_210506_WEB.pdf>]

# 8. Informationssäkerhetsrutiner för anslutning till Kanta-tjänsterna och användning av dem

[**Föreskrift 3/2024**: 6.12 Informationssäkerhetsrutiner för anslutning till Kanta-tjänsterna och användning av dem]

[Följande punkter kan också beskrivas i samband med motsvarande punkter i tidigare kapitel eller systemspecifikt]

[Jfr kapitel 6.5 i föreskrift 3/2024 om bl.a. användningsändamål för informationssystem]

I fråga om Kanta-tjänsterna iakttas följande informationssäkerhetsrutiner och rutiner för behandling av kunduppgifter:

[Aktuella beskrivningar av följande eller hänvisningar till aktuella beskrivningar:

* hur användarna utbildas eller introduceras i Kanta-tjänsterna och hur man säkerställer att de används på ett informationssäkert sätt, till exempel introduktionsmaterial, webbskolor/enkäter osv., och hur man säkerställer att introduktionen har genomförts, anvisningar till personalen (bland annat att utan dröjsmål skicka uppgifter till Kanta-tjänsterna), information till kunderna
* verksamhetsmodeller för aktiv uppföljning av användningen av Kanta-tjänsterna samt förändringssituationer
* tjänstetillhandahållarens och apotekets ansvariga parter vid störningar
* genomförande av de identifierings- och verifieringslösningar som Kanta-tjänsterna förutsätter: inloggningsrutiner för system som använder Kanta-tjänsterna
* granskning av uppgifter i organisationsregistret för social- och hälsovården eller IAH-kodsystemet:
	+ organisationer granskar uppgifterna i organisationsregistret för social- och hälsovården i den nationella kodtjänsten
	+ självständiga yrkesutövare granskar uppgifterna i IAH-kodsystemet
	+ korrigeringar av felaktiga uppgifter och tillägg meddelas alltid till det egna regionförvaltningsverket eller Valvira
	+ även uppdateringar som görs vid förändringar ska beaktas
* genomförande av de certifikatlösningar som Kanta-tjänsterna förutsätter (olika typer av yrkeskort för personalen som beställs från Myndigheten för digitalisering och befolkningsdata och servercertifikat för datatekniska tjänster)
* hantering av de åtkomsträttigheter/behörigheter som Kanta-tjänsterna förutsätter och koppling av dem till de anställdas arbetsroller – vid behov även rättigheter och uppgifter i anslutning till följande roller: administratör, arkivarie, dataskyddsombud
* uppföljning av användningen av Kanta-tjänsterna och system som ansluter till dem, inklusive uppföljning av loggen över användning och utlämnande av klientuppgifter inom socialvården och patientuppgifter: vem/vilka följer upp, på vilket sätt, hur ofta
* genomförande av Kanta-tjänsternas åtkomsthantering i de informationssystem som används
* hur man har skiljt åt socialvårdens och hälso- och sjukvårdens dokument och olika register
* på vilket sätt och hur ofta man säkerställer att de informationssystem som ansluts till Kanta-tjänsterna (i synnerhet system i klass A2 eller A3) och andra informationssystem och annan informationsförmedlingsservice som kräver certifiering (system i klass A1) har ett giltigt intyg över bedömning av informationssäkerheten och att det finns uppgifter om dem i Valviras register över informationssystem (system i klass A1, A2 eller A3). Om välbefinnandeapplikationer används i tjänstetillhandahållarens verksamhet, ska motsvarande säkerställanden göras även i fråga om dem
* på vilket sätt och hur ofta man säkerställer att informationssystemen i klass A överensstämmer med kraven med hjälp av Valviras register över informationssystem och uppgifter från producenterna av informationssystemtjänster (bland annat informationssäkerhetsintygets giltighet, profilerna för väsentliga krav som implementerats i systemet och hur samtestningarna av system som är anslutna till Kanta-tjänsterna motsvarar de specifikationer som Kanta-tjänsterna kräver) Om välbefinnandeapplikationer används i tjänstetillhandahållarens verksamhet, ska motsvarande säkerställanden göras även i fråga om dem
* på vilket sätt och hur ofta man säkerställer att övriga informationssystem som är avsedda för behandling av klientuppgifter inom socialvården eller patientuppgifter har anmälts till Valvira och att uppgifterna om dem är uppdaterade i Valviras register över informationssystem (system i klass B)
* hur man säkerställer att ett system som ska upphandlas eller uppdateras uppfyller de väsentliga krav som ställs på systemet (hur detta beskrivs i avtalen, vilka kontroller som görs till exempel av THL:s föreskrifter, systemprofiler och det intyg över bedömning av informationssäkerheten som systemet förutsätts ha, Valviras register över informationssystem och resultaten av FPA:s samtestning). Om välbefinnandeapplikationer används i tjänstetillhandahållarens verksamhet, ska motsvarande säkerställanden göras även i fråga om dem
* åtgärder och ansvar i en situation där intyget över bedömning av informationssäkerheten för ett system som används återkallas för viss tid eller helt eller begränsas eller i en situation där användningen av ett informationssystem förbjuds, beskrivning av hur detta beaktas i avtalen. Om välbefinnandeapplikationer används i tjänstetillhandahållarens verksamhet, ska motsvarande säkerställanden göras även i fråga om dem.]

# 9. Närmare beskrivningar, anvisningar och planer för varje informationssystem

[**Föreskrift 3/2024**: 6.5 Informationssystemens basuppgifter och närmare beskrivningar]

[Närmare beskrivningar av informationssystemen och deras **användningsändamål**: jfr kapitel 6.1 i mallen, Informationssystemens basuppgifter]

[I kapitel 9 i informationssäkerhetsplanen beskrivs vid behov alla eller de viktigaste informationssystemen närmare, bland annat anvisningar och planer i anslutning till dem. De informationssystem som används ska beskrivas och klassificeras utifrån hur kritiska de är. Obs! Praxis för genomförande av beredskap till följd av klassificeringarna av hur kritiska informationssystemen är beskrivs i kapitel 4 i mallen.]

[Om endast ett informationssystem används behövs inte nödvändigtvis informationssystemspecifika delar. Här kan man också hänvisa till systemspecifika beskrivningar som upprätthålls separat.]

[Förutom beskrivningar av informationssystemen ska informationssäkerhetsplanen också innehålla beskrivningar av **välbefinnandeapplikationer** och andra **digitala ärendetjänster** som riktas till kunder och som används i verksamheten av objektet för egenkontroll av informationssäkerheten. (I THL:s föreskrift 4/2024, kapitel 2 Definitioner, definieras välbefinnandeapplikationer och digitala ärendetjänster som tillsammans bildar en **digital tjänst**.)[[5]](#footnote-5)]

[I de olika punkterna som beskrivs nedan kan man i tillämpliga delar använda samma slags beskrivningar som i motsvarande delar i tidigare kapitel i informationssäkerhetsplanen. I följande mallar finns en exempelmall för beskrivning av system i klass A2 och A3 (som ansluts till Kanta-tjänsterna), klass A1 (informationssystem som genomgår bedömning av informationssäkerheten av andra orsaker), klass B (övriga system avsedda för behandling av klientuppgifter inom socialvården eller patientuppgifter) och övriga system (som vid behov kan tas med i informationssäkerhetsplanen)]

[I informationssäkerhetsplanen beskrivs nödvändiga underkapitel i enlighet med de informationssystem som används i objektet för egenkontroll av informationssäkerheten. Om egenkontrollobjektet inte har några system för ett visst underkapitel kan kapitlet strykas helt. Symbolerna X, Y och Z i underkapitlen beskriver systemen som hör till den klass eller de klasser som anges i mallens underkapitel (X1, X2; Y1, Y2; Z1, Z2). För varje system utarbetas egna beskrivningar enligt mallen i det aktuella underkapitlet.]

## 9.1 System X (hör till klass A2 och A3)

* system / välbefinnandeapplikation, version, leverantör, kontaktuppgifter: [finns delvis också i Valviras register över informationssystem, klass A]
* användningsändamål: [beskrivningen finns också i Valviras register över informationssystem, klass A]
* användargrupper:

[Följande punkter till behövliga och tillämpliga delar, om de avviker från de rutiner som beskrivs i informationssäkerhetsplanens övriga kapitel]

* bruksanvisningar:
* uppdatering och distribution av anvisningarna:
* förfaranden vid fel och problem:
* systemspecifika stödtjänster:
* ansvar och krav för installation och drift:
* tillvägagångssätt och ansvar vid fel och exceptionella situationer:
* behörighetshantering i systemet:
* identifiering i systemet:
* loggar:
* låsning av systemet:
* säkerställande av uppgifterna i intyget över bedömning av informationssäkerheten för system som ansluts till Kanta (klass A):
* uppgifter om systemet på sidan för FPA:s testresultat (klass A):
* uppgifter om systemet i Valviras register över informationssystem:
	+ tidpunkt för granskning av uppgifterna om informationssystemet i Valviras register över informationssystem
	+ datum då informationssystemets informationssäkerhetsintyg upphör att gälla
	+ de profiler för väsentliga krav som implementerats i informationssystemet
	+ FPA:s samtestningar med Kanta-tjänsterna som informationssystemet genomgått med godkänt resultat (från Valviras register över informationssystem och/eller FPA:s sida över testresultat)
	+ eventuella uppgifter i Valviras register över informationssystem om sådant som ska beaktas när informationssystemen används eller tas i bruk

## 9.2 System X (hör till klass A1)

* system / välbefinnandeapplikation, version, leverantör, kontaktuppgifter: [finns delvis också i Valviras register över informationssystem, klass A]
* användningsändamål: [beskrivningen finns också i Valviras register över informationssystem, klass A]
* användargrupper:

[Följande punkter till behövliga och tillämpliga delar, om de avviker från de rutiner som beskrivs i informationssäkerhetsplanens övriga kapitel]

* bruksanvisningar:
* uppdatering och distribution av anvisningarna:
* förfaranden vid fel och problem:
* systemspecifika stödtjänster:
* ansvar och krav för installation och drift:
* tillvägagångssätt och ansvar vid fel och exceptionella situationer:
* behörighetshantering i systemet:
* identifiering i systemet:
* loggar:
* låsning av systemet:
* säkerställande av uppgifterna i intyget över bedömning av informationssäkerheten för system som hör till klass A1:
* uppgifter om systemet på sidan för FPA:s testresultat (klass A):
* uppgifter om systemet i Valviras register över informationssystem:
	+ tidpunkt för granskning av uppgifterna om informationssystemet i Valviras register över informationssystem
	+ datum då informationssystemets informationssäkerhetsintyg upphör att gälla
	+ de profiler för väsentliga krav som implementerats i informationssystemet
	+ eventuella omnämnanden om att systemet deltar i samtestning som en del av en större informationssystemhelhet (från Valviras register över informationssystem och/eller FPA:s sida över testresultat)
	+ eventuella uppgifter i Valviras register över informationssystem om sådant som ska beaktas när informationssystemen används eller tas i bruk

## 9.3 System Y (hör till klass B)

* system (även vid behov uppgifter om sådana digitala ärendetjänster som är relaterade till den egna verksamheten), version, leverantör, kontaktuppgifter: [finns delvis också i Valviras register över informationssystem, klass B]
* användningsändamål: [beskrivningen finns också i Valviras register över informationssystem, klass B]
* användargrupper:

[Följande punkter till behövliga och tillämpliga delar, om de avviker från de rutiner som beskrivs i informationssäkerhetsplanens övriga kapitel]

* bruksanvisningar:
* uppdatering och distribution av anvisningarna:
* förfaranden vid fel och problem:
* systemspecifika stödtjänster:
* ansvar och krav för installation och drift:
* tillvägagångssätt och ansvar vid fel och exceptionella situationer:
* behörighetshantering i systemet:
* identifiering i systemet:
* loggar:
* låsning av systemet:
* uppgifter om systemet i Valviras register över informationssystem:
	+ tidpunkt för granskning av uppgifterna om informationssystemet i Valviras register över informationssystem
	+ de profiler för väsentliga krav som implementerats i informationssystemet
	+ eventuella uppgifter i Valviras register över informationssystem om sådant som ska beaktas när informationssystemen används eller tas i bruk

## 9.4 System Z (övriga system som inte hör till klass A eller B)

* system (även vid behov uppgifter om sådana digitala ärendetjänster som är relaterade till den egna verksamheten), version, leverantör, kontaktuppgifter:
* användningsändamål:
* användargrupper:

[Följande punkter till behövliga och tillämpliga delar, om de avviker från de rutiner som beskrivs i informationssäkerhetsplanens övriga kapitel]

* bruksanvisningar:
* uppdatering och distribution av anvisningarna:
* förfaranden vid fel och problem:
* systemspecifika stödtjänster:
* ansvar och krav för installation och drift:
* tillvägagångssätt och ansvar vid fel och exceptionella situationer:
* behörighetshantering i systemet:
* identifiering i systemet:
* loggar:
* låsning av systemet:
1. [Lagen om behandling av kunduppgifter inom social- och hälsovården 703/2023 (lagen om kunduppgifter), 77 §](https://www.finlex.fi/sv/laki/alkup/2023/20230703#Pidm46651394591600) [↑](#footnote-ref-1)
2. [Lagen om kunduppgifter 703/2023](https://www.finlex.fi/sv/laki/alkup/2023/20230703) [↑](#footnote-ref-2)
3. Dataombudsmannens byrå: [Register över behandling](https://tietosuoja.fi/sv/register-over-behandling) [↑](#footnote-ref-3)
4. Digital tjänst: den allmänna termen digital tjänst används i föreskrifterna 4/2024 och 5/2024 med hänvisning till både välbefinnandeapplikationer och digitala ärendetjänster. Termen omfattar både informationssystem och välbefinnandeapplikationer med egenskaper som är avsedda att vara direkt tillgängliga för medborgarna. Till de digitala tjänsterna kan räknas både digitala ärendetjänster och sådana välbefinnandeapplikationer som är anslutna till Kanta-tjänster såsom datalagret för egna uppgifter. Det är också möjligt att en digital tjänst uppfyller definitionen av både välbefinnandeapplikation och informationssystem i lagen om kunduppgifter. [↑](#footnote-ref-4)
5. Digital tjänst: den allmänna termen digital tjänst används i föreskrifterna 4/2024 och 5/2024 med hänvisning till både välbefinnandeapplikationer och digitala ärendetjänster. Termen omfattar både informationssystem och välbefinnandeapplikationer med egenskaper som är avsedda att vara direkt tillgängliga för medborgarna. Till de digitala tjänsterna kan räknas både digitala ärendetjänster och sådana välbefinnandeapplikationer som är anslutna till Kanta-tjänster såsom datalagret för egna uppgifter. Det är också möjligt att en digital tjänst uppfyller definitionen av både välbefinnandeapplikation och informationssystem i lagen om kunduppgifter. [↑](#footnote-ref-5)