Informationssikkerhedspolitik for Competencehouse.

1. Målsætning

Sikkerhedspolitikken skal til enhver tid understøtte Competencehouses værdigrundlag og vision samt de strategiske mål, der er i IT-strategien samt sikre, at Competencehouse lever op til bestemmelserne i databeskyttelsesforordningen (GDPR). Competencehouse benævnes i det følgende CH.

Det er CH's mål at udbygge sit IT-sikkerhedsniveau, så det kommer på højde med ISO 27001, som bl.a. er sikkerhedsstandarden for statslige myndigheder. Som et led i dette arbejde er CH's informationssikkerhed – herunder GoDialog – analyseret og holdt op imod gældende sikkerhedsstandarder i et eksamensprojekt i forårssemesteret 2019 på DTU. Eksamensprojektet resulterede i anbefalinger til udbygning af IT-sikkerhedsniveauet, som var implementeret ved udgangen af 2019.

Fastholdelse og udbygning af et højt sikkerhedsniveau er en væsentlig forudsætning for, at CH fremstår troværdig.

For at fastholde CH's troværdighed skal det sikres, at information behandles med fornøden fortrolighed, og at der sker fuldstændig, nøjagtig og rettidig behandling af godkendte transaktioner.

IT-systemet GoDialog betragtes, næst efter medarbejderne, som CH's mest kritiske ressource. Der lægges derfor vægt på driftssikkerhed, kvalitet, overholdelse af lovgivningskrav, og på at GoDialog er brugervenligt, dvs. uden unødigt besværlige sikkerhedsforanstaltninger.

Der skal skabes et effektivt værn mod IT-sikkerhedsmæssige trusler, således at CH's kunder samt medarbejdernes tryghed og arbejdsvilkår sikres bedst muligt. Beskyttelsen skal være vendt imod såvel naturgivne som tekniske og menneskeskabte trusler. Alle personer betragtes som værende mulig årsag til brud på sikkerheden; dvs. at ingen persongruppe skal være hævet over sikkerhedsbestemmelserne.

Målene for GoDialog er at sikre:

1. Høj driftssikkerhed med høje oppetidsprocenter og minimeret risiko for større nedbrud og datatab (tilgængelighed).
2. Korrekt funktion af GoDialog med minimeret risiko for manipulation af og fejl i såvel data som systemer (integritet).
3. Fortrolig behandling, transmission og opbevaring af data (fortrolighed).
4. Gensidig sikkerhed omkring de involverede parter (adgangskontrol).

Målene er indarbejdet i programmeringen og den driftsmæssige afvikling af GoDialog. Mål 1 og 2 er desuden indarbejdet i GoDialogs servicekatalog. Mål 3 indgår endvidere i CH's databehandleraftaler med sine kunder og i medarbejdernes persondataerklæringer.

Regler og retningslinjer fra informationssikkerhedspolitikken indarbejdes løbende i CH's persondataerklæringer, som alle ledere og medarbejdere underskriver.

2. Gyldighedsområde

Politikken er gældende for alle CH's informationsrelaterede aktiviteter, uanset om disse udføres af ansatte i CH eller af samarbejdspartnere. Aktiviteterne kan omfatte, men er ikke begrænset til at omfatte faktuelle oplysninger, optegnelser, registreringer, rapporter, forudsætninger for planlægning eller anden information, som kun er til intern brug.

Informationssikkerhedspolitikken har gyldighed for alle ansatte i CH og al anvendelse af CH's informationsaktiver.

3. Sikkerhedsmæssige foranstaltninger

Mål for åbningstid, driftseffektivitet, svartider samt procedure for mangelafhjælpning fremgår af Servicekatalog GoDialog, som alle CH's kunder har adgang til.

Adgang til GoDialog er beskyttet af brugernavn og adgangskode og hos visse kunder ved Single Sign-On (SSO).

Ved opsætningen af GoDialog tager den enkelte kunde for kundens version af GoDialog stilling til, hvilke persondata hhv. HR/administratorer, ledere og medarbejdere skal have adgang til og hvilke brugergrupper, der skal have adgang til hvilke persondata.

CH's medarbejdere må ikke ændre en kundes persondataadgangstilladelser uden forudgående skriftlig anmodning herom fra kundens HR-ansvarlige.

De persondata, som CH behandler for en kunde, fremgår af kundens databehandleraftale.

4. Backup

XDC-gruppen tager daglig backup af den virtuelle driftsserver inklusive databaseserveren (der også ligger på driftsserveren). Backupper gemmes og den enkelte backup overskrives med en ny efter 30 dage.

Backupsystemet indeholder en facilitet, der tester, om den enkelte backup er gemt korrekt. I supplement hertil foretages mindst én gang årligt et forsøg på en genindlæsning (restore) af backuppen, hvor det undersøges, om den genindlæste backup kan fungere som en server.

5. Organisation og ansvar

Jan Buch har det overordnede sikkerhedsansvar.

Thomas Krag har ansvar for den sikkerhed, der er knyttet til GoDialog, herunder for sikkerheden i de ydelser, som XDC-gruppen leverer til CH.

Jan Buch har specifikt ansvar for:

- at informationssikkerhedspolitikken er kendt og efterleves.
- at der ved installation af nye systemer gennemføres en forudgående sikkerheds/risikovurdering.
- at revidere informationssikkerhedspolitikken.

- at forebygge sikkerhedsbrud på CH's lokaler, CH's computere og andre elektroniske devices og på CH's interne netværk.
- at alle CH's kunder får databehandleraftaler.
- at CH har databehandleraftaler fra de leverandører, der har adgang til GoDialog og/eller behandler persondata om CH's kunder og/eller behandler persondata om CH's ansatte
- at al arkivering af persondata sker efter retningslinjerne i CH's privatlivsbeskyttelsespolitik.
- at alle CH's computere er indstillet til automatisk aflåsning efter 5 minutter uden brug.
- at alle adgangskoder til CH's computere kun kan tilgås med et personligt password bestående af mindst 12 karakterer (små/store bogstaver og mindst et tal eller specialtegn). Der er krav om nyt password hvert kvartal. Disse passwords kan ikke nå at brydes, inden de tvungent skiftes efter 90 dage.
- at alene CH's computere anvendes til behandling af personfølsomme data fra GoDialog.
- at alle ansatte har underskrevet en opdateret persondataerklæring.
- at der foretages opfølgning på og rapportering af sikkerhedsbrud til bestyrelsen
- at rapportere kritiske sikkerhedsbrud til Datatilsynet.
- at bortskaffe al IT-udstyr på en sikker måde.

Thomas Krag har specifikt ansvar for:

- at forebygge sikkerhedsbrud på GoDialog.
- at der foretages opfølgning på og rapportering af sikkerhedsbrud på GoDialog til direktion og berørte kunder.
- at der foretages opfølgning på og rapportering af sikkerhedsbrud hos vores hostingleverandører til direktion og berørte kunder.
- at Backup fungerer.
- at udskifte adgangskoder til superadministratorindgangen til GoDialog hvert kvartal.
- at udskifte adgangskoder til CH's servere hvert kvartal.
- at der sker en logning af, hvem der logger på som superadministrator.
- at der sker en logning af, hvem der logger på serveren.

Alle ansatte har ansvar for:

- at overholde informationssikkerhedspolitikken og de regler, der er relevante for den enkeltes arbejdsopgaver.
- at gennemlæse og underskrive den persondataerklæring, som CH udleverer.
- at påse, at de CH-computere, der arbejdes på, er indstillet efter CH's retningslinjer for automatisk aflåsning.
- at låse sine computere, når de ikke selv har dem under opsyn.
- at opdatere egne adgangskoder til sine CH-computere og e-mail hvert kvartal.
- at straks-rapportere mistanke om kunders evt. ulovlige behandling af persondata på GoDialog til Thomas Krag og direktionen.
- at straks-rapportere eventuelle sikkerhedsbrud eller mistanke herom relateret til GoDialog til Thomas Krag.
- at straks-rapportere eventuelle andre sikkerhedsbrud eller mistanke herom til Jan Buch.
- at sikre at en kundes ønske om at ændre adgangen til persondata efter kontraktindgåelse kun må ske efter forudgående skriftlig anmodning herom fra kundens HR-ansvarlige, og at arkivere den skriftlige anmodning i kundemappen på CH's drev.
- at makulere skriftligt materiale med persondata og med oplysninger om kundeforhold.
- ikke at videregive sine nøgler til Competencehouses lokaler til andre personer end ansatte i Competencehouse.

6. Beredskabsplanlægning

Sikkerhedsbrister imødegås og effekterne begrænses ved overvågning af CH's servere og af trafikken på GoDialog.

Det forhold, at såvel kundernes data som CH's persondata ligger på eksternt placerede servere og tilgås via fjernskrivebord, minimerer risikoen for tab af persondata og at uønskede personer kan få adgang til data.

CH's servere er placeret i Danmark og overvåges af XDC-gruppen. XDC-gruppen har en ISAE 3402 type 2 erklæring. XDC-gruppen anvender eksterne, danske datacentre som underleverandører. Alle disse har som minimum også en ISAE 3402 type 2 erklæring. En evt. katastrofe, der berører GoDialogs servere, er omfattet af XDC-gruppen og dennes underleverandørers beredskabsplaner.

Den server, der afvikler GoDialog, overvåges løbende, og besked sendes både til CH og til CH's hostingleverandør ved problemer. Supplerende hermed tjekkes hvert minut, om GoDialog reagerer på en konkret forespørgsel. Er dette ikke tilfældet, modtager CH besked herom. Hermed sikres, at CH kan tage aktion i samme øjeblik, at der måtte opstå problemer med GoDialog.

Competencehouses medarbejdere arbejder ved at logge ind på et fjernskrivebord. Ved anvendelse af fjernskrivebordsadgang er det muligt for medarbejderne at arbejde i et sikret miljø. Sikkerhedsniveauet for forbindelsen er højt, da der logges ind på vores fjernskrivebord med meget stærke passwords (min. 12 karakterer, små/store bogstaver og mindst et tal eller specialtegn), der skiftes hver tredje måned samt to-faktor bekræftelse med medarbejdernes telefon. Medarbejderne har skrevet under på ikke at gemme kunderelaterede oplysninger udenfor fjernskrivebordet og er gjort opmærksomme på, at al behandling af kundedata skal foregå på fjernskrivebordet og ikke på den computer, de benytter til at forbinde til fjernskrivebordet, jvf. persondatapolitikken. Fjernforbindelsen overvåges i tilfælde af, at der overføres filer til eller fra fjernskrivebordet.

7. Sanktionering

Ansatte, der bryder de gældende informationssikkerhedsbestemmelser i CH kan straffes disciplinært, afhængig af sikkerhedsbruddets karakter med en mundtlig påtale, en mundtlig advarsel, en skriftlig advarsel, afskedigelse, bortvisning eller politianmeldelse.