Informationssikkerhedspolitik

PROFESSIONS-
HØJSKOLEN
ABSALON

Indledning

Informationssikkerhedspolitikken skal til enhver tid understøtte Professionshøjskolen Absalons værdigrundlag og vision samt de strategiske mål.

Denne informationssikkerhedspolitik er den overordnede ramme for informationssikkerheden hos Absalon. Som et led i den overordnede sikkerhedsstyring tager ledelsen på grundlag af den løbende overvågning og rapportering informationssikkerhedspolitikken op til revurdering minimum hvert andet år.

Politikken omfatter Absalons informationer, som er enhver information, der tilhører Absalon herudover også informationer, som ikke tilhører Absalon, men som Absalon kan gøres ansvarlig for. Dette inkluderer fx alle data om personale, data om finansielle forhold, alle data, som bidrager til administrationen af Absalon, samt informationer som er overladt Absalon af andre, herunder forsøgs- og forskningsdata. Disse data kan være faktuelle oplysninger, optegnelser, registreringer, rapporter, forudsætninger for planlægning eller enhver anden information, som kun er til intern brug.

Denne politik omfatter alle Absalons informationer, ligegyldigt hvilken form de opbevares og formidles på.

Formål

Informationer og informationssystemer er nødvendige og livsvigtige for Absalon, og informationssikkerheden har derfor vital betydning for Absalons troværdighed og funktionsdygtighed.

Formålet med informationssikkerhedspolitikken er at definere en ramme for beskyttelse af Absalons informationer og særligt at sikre, at kritiske og følsomme informationer og informationssystemer bevarer deres fortrolighed, integritet og tilgængelighed.

Derfor har Absalons ledelse besluttet sig for et beskyttelsesniveau, der er afstemt efter risiko og væsentlighed samt overholder lovkrav, databeskyttelsesforordningen (GDPR), databeskyttelsesloven og indgåede aftaler, herunder licensbetingelser. Ledelsen vil oplyse medarbejdere og studerende om ansvarlighed i relation til Absalons informationer og informationssystemer.

Hensigten med informationssikkerhedspolitikken er endvidere at tilkendegive over for alle, som har en relation til Absalon, at anvendelse af informationer og informationssystemer er underkastet standarder og retningslinjer. På den måde kan sikkerhedsproblemer forebygges, eventuelle skader kan begrænses, og retablering af informationer kan sikres.

Målsætning

Det er Absalons mål at opretholde et højt informationssikkerhedsniveau, der som minimum er på samme niveau som sammenlignelige institutioners. Målsætningen om et højt sikkerhedsniveau afvejes med ønsket om en hensigtsmæssig og brugervenlig anvendelse af it og øvrige økonomiske ressourcer.

Kravene til informationssikkerhed vurderes i forhold til deres relevans for Absalon, og hermed holdes fokus på et informationssikkerhedsniveau, hvor god sund fornuft samt hensynet til brugernes berettigede behov og offentlighedens forventning om en sikker forvaltning af data og aktiver er en afgørende faktor. Desuden skal data og systemer sikres ud fra en vurdering af, hvad der er nødvendigt under hensyntagen til de økonomiske rammer.

De overordnede mål for informationssikkerheden er derfor, at:

- opnå høj driftssikkerhed med høje oppetidsprocenter og minimeret risiko for større nedbrud og datatab - TILGÆNGELIGHED
- opnå korrekt funktion af systemerne med minimeret risiko for manipulation af og fejl i såvel data som systemer - INTEGRITET
- opnå fortrolig behandling, transmission og opbevaring af data - FORTROLIGHED

IT-systemer betragtes, næst efter medarbejderne, som Absalons mest kritiske ressource. Der lægges derfor vægt på driftssikkerhed, kvalitet, overholdelse af lovgivningskrav og på at systemerne er brugervenlige, dvs. uden unødigt besværlige sikkerhedsforanstaltninger.

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

Digital skal derfor understøtte informationssikkerheden til at:

- Opnå mulighed for fortrolig behandling, transmission og opbevaring af data, bl.a. ved brug af identificering/pseudonymisering og kryptering af data i størst muligt omfang.
- Opnå høj driftssikkerhed og minimal risiko for større nedbrud
- Understøtte overholdelsen af Databeskyttelsesforordningen (GDPR), også som databehandler for andre
- Forhindre datatab og -lækager
- Opnå korrekt funktion af it-systemerne med minimeret risiko for manipulation af data og systemer. Dvs. at faciliteter hertil skal være til stede og benyttes efter konkret behov
- Sikre mod forsøg på tilsidesættelse af sikringsforanstaltninger
- Understøtte bevidstheden om informationssikkerhed internt og eksternt, så alle medarbejdere og eksterne brugere er opmærksomme på og forholder sig til informationssikkerhed i det daglige arbejde.

Omfang

Informationssikkerhedspolitikkens scope og omfang defineres således til at omfatte følgende tre overordnede områder.

1. Mennesker, organisation og processer

Medarbejdernes adfærd i dagligdagen har stor betydning for informationssikkerheden. Det er centralt, at alle medarbejdere er bevidste om, hvordan deres adfærd påvirker informationssikkerheden. Det handler både om, hvordan medarbejderne håndterer teknik og it-udstyr, og om hvordan de omgås følsomme personoplysninger. Medarbejderne skal derfor have kendskab til lovgivning, organisationens egne politikker, retningslinjer og instrukser - og selvfølgelig også overholde dem. Ledelsens prioritering af området er også vigtig. Derfor skal der sikres en organisation, der prioriterer informationssikkerhed, så medarbejdere og ledelse har gode betingelser for at arbejde med følsomme personoplysninger.

2. It-systemer og fysisk sikkerhed

Absalons brug og håndtering af personoplysninger skal foregå betryggende og med et passende niveau af sikkerhed og privatlivsbeskyttelse. Det kræver blandt andet, at oplysningerne sikres tilstrækkeligt, at datas integritet bevares og at oplysningerne ikke ændres uden autorisation. Data skal kun være tilgængelige for dem, som må og skal bruge dem og det skal foregå sikkert. Dette stiller tekniske krav i forbindelse med udvikling, implementering og drift af it-løsninger og krav til den fysiske sikring af hardware og lignende.

3. Lovkrav og kontraktkrav

Absalon skal sikre, at relevante lov- og kontraktkrav overholdes i det daglige arbejde. Personoplysninger må kun behandles i tilfælde, hvor et legitimt formål og det nødvendige lovgrundlag foreligger. Dette element af informationssikkerhed indebærer også et fokus på, at der indskrives konkrete kontraktkrav til informationssikkerhed i de drifts- og udviklingsaftaler, som Absalon indgår med leverandører.

Den politiske linje for informationssikkerhed stiller desuden krav til, at Absalon efterlever ISO 27001-standarden. Dette sker ved, at et ledelsessystem for informationssikkerhed inden for rammerne af informationssikkerhedsstandarden ISO etableres, implementeres, vedligeholder og løbende forbedres.

Denne politik gælder for alle ansatte uden undtagelse, både fastansatte og personer, som midlertidigt arbejder for Absalon. Alle disse personer bliver her betegnet som medarbejdere.

Politikken gælder endvidere for studerende, der i forbindelse med deres studie anvender informationsaktiver tilhørende Absalon.

Ved udlicitering af dele af eller hele IT-driften skal det sikres i samarbejdet med serviceleverandøren, at Absalons sikkerhedsniveau fastholdes, så serviceleverandøren, dennes faciliteter og de medarbejdere, som har adgang til Absalons informationer, mindst lever op til Absalons informationssikkerhedsniveau.

Organisering af informationssikkerhedsarbejdet

For at sikre at Absalons behandling og opbevaring af følsomme personoplysninger lever op til lovens krav er organiseringen af informationssikkerhedsarbejdet indrettet på en måde, der understøtter at informationssikkerhedsreglerne efterleves i praksis.

Det indebærer, at Absalon har organiseret sit informationssikkerhedsarbejde på tre niveauer; det strategiske niveau, det taktiske niveau og det operationelle niveau, jf. figuren nedenfor.

Planlægningen, implementeringen af og kontrollen af informationssikkerheden er defineret af Absalons ledelse (direktionen). Informationssikkerhedskoordinatoren er ansvarlig for implementering og vedligeholdelse af informationssikkerhedssystemet og for opfølgning på sikkerhedshændelser.

Det er direktionens ansvar at træffe den endelige beslutning om et sikkerhedsniveau, der er afstemt efter risiko og væsentlighed og offentlighedens interesser. Niveauet skal overholde relevante lov- og kontraktkrav.

Direktionen har ansvar for at understøtte politikker, retningslinjer og instrukser samt allokere nødvendige ressourcer til at gennemføre arbejdet med informationssikkerhed i Absalon. Og skal sikre, at medarbejderne har den fornødne viden om informationssikkerhed.

Informationssikkerhedsudvalget (ISU) har til opgave at "oversætte" direktionens overordnede retningslinjer for, hvordan sikkerhedsbehovet kan opfyldes, så cheferne for afdelinger og centre kan sikre, at disse efterleves i egne enheder.

Ledelsen skal arbejde for en kultur, hvor ansvarlighed i forhold til informationsbehandling falder naturligt for alle. Alle medarbejdere har et ansvar for at bidrage til, at organisationens oplysninger ikkekommer i de forkerte hænder. Det er ledelsens ansvar at sikre, at alle medarbejdere har den fornødne viden om informationssikkerhed, og at der i relevant omfang sker en løbende uddannelse i

informationssikkerhed. Tilsvarende er medarbejderne forpligtede til at gøre sig bekendt med den information om informationssikkerhed, der stilles til rådighed.

Absalon har en informationssikkerhedskoordinator, som er personalemæssigt placeret i Digital, men i informationssikkerhedsmæssige spørgsmål refererer til formanden for informationssikkerhedsudvalget.

Det operationelle ansvar for den daglige styring af informationssikkerhedsindsatsen er placeret hos informationssikkerhedskoordinatoren. Denne sikrer i samarbejde med informationssikkerhedsudvalget og digitaliseringschefen, at de aktiviteter, standarder, retningslinjer, kontroller og foranstaltninger, der skal understøtte informationssikkerhedspolitikken, gennemføres og efterleves. Ligeledes er det væsentligt, at informationssikkerhed integreres i alle forretningsgange, driftsopgaver og projekter.

Absalon har udpeget systemejere, som er de fagligt ansvarlige for Absalons systemer. De skal sikre, at de gældende informationssikkerhedsregler for systemerne overholdes.

Alle medarbejdere er personligt ansvarlige for at overholde Absalons informationssikkerhedsregler og skriver under herpå ved ansættelsen.

Sikkerhedsniveau

Det er Absalons politik at beskytte sine informationer og udelukkende tillade brug, adgang og offentliggørelse af informationer i overensstemmelse med Absalons retningslinjer og under hensyntagen til den til enhver tid gældende lovgivning.

Absalon fastlægger på baggrund af en risikovurdering et sikkerhedsniveau som svarer til betydningen af de pågældende informationer.

Der gennemføres mindst en gang årligt en risikovurdering, så ledelsen kan holde sig informeret om det aktuelle risikobillede. Der foretages ligeledes en risikovurdering ved større forandringer i organisationen.

Sikkerhedsniveauet fastlægges i det enkelte tilfælde under hensyntagen til arbejdets gennemførelse og økonomiske ressourcer. Målsætningen om et højt sikkerhedsniveau afvejes med ønsket om en hensigtsmæssig og brugervenlig anvendelse af it, samt det forhold at Absalon har en samfundsrolle som leverandør af frit tilgængelig information.

Sikkerhedsbevidsthed

Informationssikkerhed vedrører Absalons samlede informationsflow. Alle medarbejdere og studerende har et ansvar for at bidrage til at beskytte Absalons informationer mod uautoriseret adgang, ændring og ødelæggelse samt tyveri. Alle medarbejdere og studerende skal derfor løbende have information om informationssikkerhed i relevant omfang.

Som brugere af Absalons informationer skal alle medarbejdere og studerende følge informationssikkerhedspolitikken og de retningslinjer, der er afledt heraf. Medarbejderne og de studerende må kun anvende Absalons informationer i overensstemmelse med det arbejde, de udfører for Absalon, og skal beskytte informationerne på en måde, som er i overensstemmelse med informationernes følsomhed, særlige og/eller kritiske natur.

Den nødvendige viden og kompetence omkring informationssikkerhed skal kommunikeres til alle medarbejdere, og der skal løbende arbejdes med holdninger, kultur og viden omkring informationssikkerhed; dette skal ske i forbindelse med ansættelsen samt løbende i form af jævnlige awareness-kampagner.

Risikovurdering

Det er Absalons politik at have en risikobaseret tilgang til informationssikkerhed jf. ISO 27001. Det vil sige, at Absalon forholder sig aktivt til hvilke risici, der eksisterer og beslutter hvilke tiltag, der skal imødegå risici.

Det er Absalons målsætning at være bevidst om relevante risici, og forholde sig til disse set i lyset af økonomiske forhold.

Risikovurderingen af Absalons kritiske systemer skal gennemføres en gang årligt, samt ved eventuelle større ændringer i opgaver, leverandører, it-systemer eller anvendelsen deraf. Inden en evt. ibrugtagning af ny teknologi, såsom Cloudbaserede systemer, skal der ligeledes gennemføres risikovurderinger.

Direktionen tager stilling til risikovurderingen og er ansvarlige for at udforme en sikkerhedsstrategi, der imødegår uacceptable risici under hensyntagen til de økonomiske forhold.

Brud på informationssikkerheden

Såfremt en medarbejder eller en studerende opdager trusler mod informationssikkerheden eller brud på denne, skal dette straks meddeles til den ansvarlige for den daglige ledelse af informationssikkerhedsindsatsen, så Absalon kan udvise god datasikkerhed ved hurtigst muligt at registrere og agere på anmeldelsen samt at lære af et eventuelt brud og derved undgå lignende sager i fremtiden.

Overtrædelse af informationssikkerhedspolitikken, eller heraf afledte regler og retningslinjer, indrapporteres til nærmeste leder, som i samarbejde med HR-afdelingen træffer afgørelse om, hvorvidt det eventuelt skal have ansættelsesretlige konsekvenser for den medarbejder, der har overtrådt reglerne. Hvis overtrædelsen er udført af en studerende, behandles sagen som enhver anden disciplinærsag.

Afvigelser og internt tilsyn

Afvigelser
Hvis der opstår situationer, hvor kravene i informationssikkerhedspolitikken ikke kan efterleves, skal der skriftligt anmodes om dispensation, stilet til Informationssikkerhedsudvalgets formand. Eventuelle afvigelser fra kravene skal dokumenteres, og der skal indføres alternative sikringsforanstaltninger.

Der tages dog højde for beredskabssituationer, hvor akutte kriser kan medføre midlertidige afvigelser, der må besluttes på stedet. Sådanne tilfælde skal efterfølgende anmeldes til Informationssikkerhedsudvalgets formand.

Internt tilsyn
Ifølge ISO 27001 er ansvaret for informationssikkerheden og dermed også for det interne tilsyn forankret hos ledelsen. Der er udpeget en overordnet ansvarlig, der i sikkerhedsspørgsmål refererer til digitaliseringschefen, og som skal etablere og vedligeholde et samlet overblik over Absalons interne tilsyn.

Det interne tilsyn skal sikre, at der sker udarbejdelse og vedligeholdelse af en overordnet plan for internt tilsyn med udgangspunkt i SoA-dokumentet. Desuden skal tilsynet sikre, at de interne tilsyn gennemføres med de angivne intervaller for hver SoA kontrol, at de dokumenteres og at der sker opfølgning på resultaterne af tilsynene. Tilsynene er baseret på stikprøvekontroller inden for de aktuelle områder samt gennemgang og vurdering af de rapporter, der dannes på basis af den foretagne logning.

Absalons databeskyttelsesrådgiver laver internt tilsyn med efterlevelse af de dataretslige regler, samt med databehandleraftaler og leverandører, der behandler personoplysninger på vegne af professionshøjskolen.

Endelig skal det sikres, at der sker rapportering af resultaterne af de interne tilsyn til ledelsen og til Informationssikkerhedsudvalget ved de ordinære og evt. ekstraordinære møder.

Informationssikkerhedskoordinatoren er udpeget som ansvarlig for planlægning af det interne tilsyn.

Afvigelser, der konstateres i forbindelse med gennemførelse af det interne tilsyn, registreres og behandles i sammenhæng med den øvrige risikostyring.

Opfølgning

Absalon monitorerer, vurderer og følger op på informationssikkerhedsområdet på følgende måde:

- Absalon følger op på informationssikkerheden ved fortsat at optimere ledelsessystemet igennem løbende vedligehold og optimering af informationssikkerhedspolitikken og de

dertilhørende regler og procedurer. Målet er, at sikre en struktureret og kontinuerlig forbedringsproces.
- Der foretages en årlig risikovurdering, hvor der efter behov inddrages uvildige eksterne konsulenter.
- Der foretages en løbende sårbarhedsscanning af Absalons eksternt rettede systemer med henblik på at identificere eventuelle risici for systemindtrængning mv.
- Der sker en løbende registrering og opfølgning på hændelser inden for informationssikkerhedsområdet.

Vedligehold og ikrafttrædelse

Håndtering af ændringer i sikkerhedsdokumentationen foretages på følgende måde:

1. Informationssikkerhedspolitikken skal godkendes af Informationssikkerhedsudvalget og direktionen. Politikken vedligeholdes med jævne mellemrum, hvilket som minimum er hvert andet år.
2. Væsentlige procedurer skal gennemses og vedligeholdes med jævne mellemrum.
3. Operationelle procedurer vedligeholdes og godkendes af informationssikkerhedskoordinatoren.

Informationssikkerhedspolitikken er godkendt af direktionen den 5. november samt på Informationssikkerhedsudvalgets møde den 12. november 2019, hvorefter den er trådt i kraft.