IT-sikkerhedspolitik

for SOSU Esbjerg

Indhold

IT-sikkerhedspolitik

Formål

Skolens IT-sikkerhedspolitik udgør den overordnede ramme for at opretholde it-sikkerheden hos SOSU Esbjerg og tager afsæt i de vigtigste krav i EU's generelle persondataforordning.

Formålet med IT-sikkerhedspolitikken er at sikre:

• Fortrolighed, integritet og tilgængelighed af persondata i overensstemmelse med kravene i EU's persondataforordning

• Høj driftssikkerhed og minimeret risiko for større nedbrud og tab af data

IT-sikkerhedspolitikken hører sammen med Social og Sundhedsskolens overordnede Persondatapolitik og uddybes desuden gennem konkrete procedurer og vejledninger.

Grundprincipper for sikkerhedsarbejdet

Funktionsadskillelse og adgangsstyring

Skolens ledelse vedtager principper for, hvilke arbejdsfunktioner der skal have adgang til hvilke funktioner i hvilke systemer. Heri ligger begrænsning i adgangen til specifikke systemer og data ved at definere brugerroller og ved at tildele privilegerede adgangsrettigheder. Disse rettigheder tildeles af en IT-kyndig medarbejder på baggrund af procedurer for brugerregistrering og -afmelding samt for tildeling af Brugeradgange - vedtaget af ledelsen.

Skolen gennemgår og ajourfører i en fast rutine tildelte rettigheder for at konstatere, om de fortsat er gældende og i overensstemmelse med den ansattes arbejdsområde.

Sikkerhedsforanstaltninger

Skolen har et samarbejde med IT Center Nord, der står for den tekniske sikkerhed. Dette sker med baggrund i IT Center Nords beskrivelse 'IT-Sikkerhedspolitik' af januar 2021, der i vid udstrækning danner udgangspunkt for sikkerhedsarbejdet.

IT Center Nord iværksætter og installerer således de nødvendige tekniske sikkerhedsforanstaltninger jf. Databehandleraftale mellem SOSU Esbjerg (dataansvarlige) og IT Center Nord (databehandleren). SOSU Esbjerg følger de beskrevne sikkerhedsforanstaltninger i Databehandleraftalens bilag C.2. som også kan ses sidst i nærværende IT-sikkerhedspolitik som bilag 1.

Skolen udarbejder administrative retningslinjer, procedurer og instrukser.

Styring af sikkerhedshændelser

Skolen sikrer løbende en vurdering af eventuelle hændelser, der kan true sikkerheden.

Databrud meldes til Datatilsynet indenfor 72 timer efter gældende regler, ligesom bestyrelsen orienteres om hændelser, der måtte være sket og hvilke tiltag, der er sat i værk for at imødegå databruddet og afbøde konsekvenserne. Der er udarbejdet procedure herfor.

Databrud, tiltag og underretninger dokumenteres og journaliseres.

Sikkerhed i forbindelse med brug af databehandlere

Leverandører, der helt eller delvist står for drift af skolens systemer, skal overholde skolens krav til it-sikkerhed.

De skal også sikre, at der er mulighed for løbende at kunne kontrollere og følge op på deres sikringsforanstaltninger.

I forbindelse med at der bliver indgået en kontrakt om at behandle data på skolens vegne, udarbejdes der en databehandleraftale med afsæt i Datatilsynets vejledning om databehandleraftaler. I databehandleraftalen beskrives i detaljer de sikkerhedskrav, som leverandøren skal leve op til.

Skolen følger op én gang årligt, at leverandører kan dokumentere at it-sikkerheden er i orden, fx, ved aflevering af en revisionserklæring eller lignende.

Organisering af sikkerhedsarbejdet

Bestyrelsen er ansvarlig for den overordnede it-sikkerhed samt for udformning af en it-sikkerhedspolitik.

Det er direktøren, der beslutter hvem, der skal have adgang til hvilke it-ressourcer og hvornår. Direktøren står til ansvar for dette over for bestyrelsen. En udpeget it-ansvarlig installerer rettigheder/begrænsninger i overensstemmelse med disse beslutninger, jf. afsnittet om funktionsadskillelse og adgangsstyring.

Styringen sker i en proces, hvor der gennemføres risikovurdering, målfastlæggelse, planlægning, gennemførelse, overvågning og opfølgning – i en tilbagevendende cyklus.

Skolen sikrer kontinuerlig kvalitetsopfølgning på overholdelse af IT-sikkerhedspolitikken i en fast rytme.

Medarbejdersikkerhed

Medarbejderne informeres om krav om it-sikkerhed før og under ansættelsen samt efter ansættelsens ophør eller ændring. Specielt er der særlige sikkerhedskrav forbundet med arbejde i hjemmet.

Skolen sikrer en løbende information og vejledning af medarbejderne om såvel IT-sikkerhedspolitikken, persondatapolitikken som andre forhold omkring håndtering af persondata på skolen.

Skolen følger overholdelse af procedurer og retningslinjer gennem løbende kvalitetsopfølgning.

Styring af medier/aktiver

Skolens it-aktiver (software, data, eller fysiske enheder) identificeres og registreres. For hvert aktiv udpeges en 'ejer', således at denne har ansvaret for korrekt håndtering af det enkelte aktiv/medie.

Bortskaffelse af medier: Medier, som indeholder fortrolig information, skal lagres og bortskaffes forsvarligt, for eksempel ved ødelæggelse, makulering, eller sletning af data.

Transport af fysiske medier: Medier med fortrolig information skal beskyttes mod uautoriseret adgang, misbrug eller ødelæggelse under transport. Dette gælder også bærbare computere, tablets og mobiltelefoner.

Sikring af fysiske personoplysninger

Skolen anvender som hovedregel digitale arbejdsgange. Derved minimeres fysiske personoplysninger. Når disse ikke kan undgås, opbevares og transporteres de forsvarligt og destrueres efter brug.

Driftsikkerhed

Driftssikkerhed drejer sig om at opnå korrekt og sikker drift af faciliteterne, der behandler information.

Heri indgår dokumentering af procedurer for drift og softwareinstallation samt styring af de ændringer, der løbende forekommer og som kan påvirke informationssikkerheden.

Endvidere skal der indføres sikkerhedsforanstaltninger, der kan opdage og forhindre sikkerhedsbrud forårsaget af malware samt efterfølgende sikre genstart af driftssystemerne.

For at sikre at al væsentlig information, software og systemer kan genskabes efter et nedbrud/sikkerhedsbrud, skal der foreligge en backupplan, som følges i praksis. Endelig skal der, hvor det er muligt, gennemføres løbende logning og overvågning af brugeraktivitet med henblik på, at kunne dokumentere hændelsesforløbet i forbindelse med et sikkerhedsbrud.

Der henvises til samarbejdet med IT Center Nord og 'IT-sikkerhedspolitik ' niveau 1, 2 og 3 samt Basis Service Level Agreement for overvågning, sikkerhed og logning jfr. bilag 1 i samarbejdsaftalen.

Kommunikationssikkerhed

Skolens interne netværk/ drev styres og overvåges og har installeret passende sikkerhedsforanstaltninger.

Ved overførsel af informationer til eksterne samarbejdspartnere skal der gøres særlige overvejelser om hvilket sikkerhedsniveau, der skal benyttes.

Via IT Center Nord er der etableret sikker mail på skolen, og for følsomme oplysninger er der mulighed for at sende mails via en OME-løsning med skærpet sikkerhed. Ved kommunikation med kommuner er der ofte behov for at kommunikere med såvel kryptering som signering. Dette sker ved vedligeholdelse af certifikat.

Skolen sikrer en løbende information og vejledning af medarbejderne om kommunikationssikkerhed og brug af sikre kommunikationslinjer. Skolen følger kommunikationssikkerheden gennem løbende kvalitetsopfølgning.

Anskaffelse, udvikling og vedligeholdelse af systemer samt leverandørforhold

Sikkerhed indgår som en integreret del af de systemer, der understøtter skolens daglige drift. Det vil sige, at krav til sikkerhed skal specificeres i forbindelse med anskaffelse, udvikling og vedligeholdelse af systemerne.

Sikkerhedskravene skal være begrundede, aftalte og dokumenterede. Formulering af sikkerhedskravene sker på basis af en risikovurdering.

Brug af databehandlere skal være baseret på en kontrakt samt en databehandleraftale, som sikrer, at skolens it-sikkerhedspolitik ikke skades. Aftalen skal indeholde principielle og konkrete krav til it-sikkerheden hos leverandøren, samt til hvordan kommunikationen mellem skolen og leverandøren skal sikres. Der skal leveres revisorerklæringer om it-sikkerheden og gives mulighed for inspektion af it-sikkerheden i særlige situationer (kontraktligt aftalt).

It-udstyr, der kobler sig på skolens systemer via eksterne netværk, skal overholde skolens sikkerhedspolitik og –retningslinjer.

Databeskyttelsesrådgiver - DPO

Skolen har som offentlig myndighed udpeget en DPO, der arbejder efter Datatilsynets vejledning om Databeskyttelsesrådgivere.

Kontaktoplysninger:

Anne-Lene Pugholm

Adresse: Øster Uttrup Vej 1, 9000 Aalborg

CVR: 46994051

Tlf: 2526 6975 /7250 5975

E-mail: alpu@itcn.dk

Website: www.itcn.dk

Vejledninger i tilslutning til denne politik

Retningslinje for håndtering af brud på persondatasikkerheden

Vejledning om hjemmearbejdspladser

Vejledning om TV-overvågning.

Vejledning i oprettelse af krypteret mailkorrespondance fra ekstern kilde.

Procedure for beredskab ved brud på persondatasikkerheden ver. 1.1

Beredskabsplan til håndtering af sikkerhedsbrist jf. Persondataforordningen (ITCenter Nord)

IT-sikkerhedspolitik – niveau 1 – (krav) (ITCenter Nord)

IT-sikkerhedspolitik – niveau 2 – IT- procedure og sikkerhedspolitik (Hvad) (ITCenter Nord)

IT-sikkerhedspolitik – niveau 3 – Opgaver vedrørende IT-procedure og sikkerhedsinstruks (Hvordan) (ITCenter Nord)

Vejledning for IT- adfærd ved SOSU Esbjerg.

Databehandleraftale mellem SOSU Esbjerg og IT Center Nord

Produktkatalog_sikkerhed

Kilder

EU's persondataforordning
http://eur-lex.europa.eu/legal-content/DA/TXT/?uri=uri-serv:OJ.L_.2016.119.01.0001.01.DAN&toc=OJ:L:2016:119:TOC

IT Center Nord – IT-sikkerhedspolitik niveau 1, 2 og 3 – herunder sikkerhedsinstruks

Datatilsynets vejledning om Databeskyttelsesrådgivere
https://www.datatilsynet.dk/media/6561/databeskyttelsesraadgivere.pdf

Bilag 1

Bilag 2C fra Databehandleraftalen mellem IT Center Nord og SOSU Esbjerg.

C.2. Behandlingssikkerhed Sikkerhedsniveauet skal afspejle:

• Sikkerhedsniveauet afspejler at der er tale om både almindelige personoplysninger omfattet af Persondataforordningens artikel 5 og særlige kategorier af personoplysninger omfattet af Persondataforordningens artikel 9 og 10.

• Databehandleren er herefter berettiget og forpligtet til at træffe beslutninger om, hvilke tekniske og organisatoriske sikkerhedsforanstaltninger, der skal anvendes for at skabe det nødvendige (og aftalte) sikkerhedsniveau omkring oplysningerne.

• Databehandleren skal dog – i alle tilfælde og som minimum – gennemføre følgende foranstaltninger, som er aftalt med den dataansvarlige.

Se i øvrigt IT Center Nord's ISAE 3402 Type 2 og ISAE 3000 erklæring.

Databehandleren er herefter berettiget og forpligtet til at træffe beslutninger om, hvilke tekniske og organisatoriske sikkerhedsforanstaltninger, der skal gennemføres for at etableret det nødvendige (og aftalte) sikkerhedsniveau.

Databehandleren skal dog – under alle omstændigheder og som minimum – gennemføre følgende foranstaltninger, som er aftalt med den dataansvarlige:

Risikovurdering

IT Center Nord benytter sig af en risikobaseret tilgang til beskyttelse af Persondata. Risikoen er vurderet fra de registreredes synspunkt, og de mitigerende foranstaltninger afspejler, at risikoen for de registrerede skal mindskes.

Antivirus og Firewall

Til beskyttelse mod virus og anden malware findes en procedure, der sikrer, at der installeres Antivirus og Firewall på alle domain PC'er. Proceduren er automatisk, og der kan ikke kobles på IT Center Nords domain, medmindre der er installeret Antivirus og Firewall og disse er aktive.Standardkontraktsbestemmelser januar 2020 For yderligere at beskytte persondata har IT Center Nord procedurer, der sikrer, at der altid Side 15 af 18 er en opdateret Firewall installeret. Firewallen beskytter mod indtrængen i IT Center Nords netværk udefra.

Segmentering af netværk

IT Center Nord har en procedure, som sikrer, at alle Dataansvarliges netværk er segmenteret så f.eks. elever ikke kan få adgang til skolens administrative systemer og data.

Bruger administration

Den daglige brugeradministration af medarbejdere er administreret af centrale it-medarbejdere i IT Center Nord. Der udføres kun oprettelser og nedlæggelser af medarbejdere efter henvendelse fra HR-afdelingen

eller den af HR-afdelingen udpegede medarbejder, til den enkelte institution i de tilfælde, hvor oprettelserne er manuelle. Oprettelser og nedlæggelser sker efter fastlagte procedurer aftalt med den enkelte institution. Alle oprettelser og nedlæggelser registreres/dokumenteres i IT Center Nords Helpdesk-system.

Medarbejdere kan kun få foretaget mindre rettelser vedr. personlig information på egen henvendelse. Administrationen af sikkerhedsgrupper og medlemskaber af disse grupper foretages af centrale it-medarbejdere ved IT Center Nord og kun på foranledning af en sag i Helpdesk.

Overvågning og logning

IT Center Nord Driftsafdeling (DRIFT) anvender i det daglige RUNNER-funktionen til at håndtere den løbende driftsafvikling og overvågning.

Logovervågning har det formål at identificere når noget unormalt sker på de enheder, som er omfattet af overvågningen. Det kan være virus, malware, forkerte opsætninger, tegn på hacking m.m.

Dette gøres ved at indsamle og overvåge relevante sikkerhedslogs for derigennem at kunne alarmere på hændelser.

Det er udelukkede logs med relevant information omkring sikkerhed på enheden, som behandles.

Process for ”alarm”:

• En potentiel sikkerhedshændelse sker på en enhed

• Sikkerhedslog genereres og fremsendes til overvågningssystemet, hvor den sammenholdes med prædefinerede ”regler”

• Konflikt med regel resulterer i, at der pr. automatik sendes en notifikation til IT Center Nord-support, f.eks. ”Password never expires”. Der sendes besked til Helpdesk om, at der er foretaget en ulovlig ændring på en brugerkonto

• Her vil der blive analyseret på, hvorfor alarmen er gået, og hvorvidt der er tale om en falsk alarm, eller om årsagen skal undersøges nærmere

• Hvis der er tale om en reel sikkerhedshændelse, vil IT Center Nord-support håndtere denne i henhold til IT Center Nords fastlagte procedurer.

Løsningen giver således mulighed for at identificere og håndtere sikkerhedshændelser og dermed øge it-sikkerheden.

Sårbarhedsskanninger og change management

Der foretages ugentlige og kvartalsvise sårbarhedsscanninger. Den ugentlige skanning udføres hver torsdag kl. 21 og varer til næste morgen. Den kvartalsvise skanning udføres på 4 Standardkontraktsbestemmelser januar 2020 specifikke søndage jævnt fordelt over året i følgende måneder: februar, maj, august og no-
 vember. Skanningen starter kl. 13 og varer ca. 12 timer.

Opdateringer og rettelser implementeres løbende.

På Windows-serverplatformen anvendes opdateringer fra Windows Update. De hentes direkte fra Microsoft og installeres automatisk, så systemet altid er helt opdateret.

På Windows arbejdsstationsplatformen anvendes opdateringer fra lokal SCCM og WSUS-server. De hentes direkte fra Microsoft og testes i en ”hotfix test group” og frigives til alle arbejdsstationer efter 7 dage.

Opdateringer på domain controllere, virtuel farm og filcluster-servere foretages forskudt, således at der ikke er nedetid for brugerne.

Opdateringer til deployerede applikationer installeres, når de frigives af producenten.

Inden større systemændringer kontrolleres det, at der forefindes en tidsvarende backup, således at der kan vendes tilbage til fungerende tilstand, hvis opdateringerne indfører fejl på systemet.

To faktor authentication Der er, hos IT Center Nords medarbejdere, indført to faktor authentication til de systemer og de enheder, hvor det er muligt.

Fysisk adgang

Adgang til serverrum er elektronisk med nøglekort og er begrænset til autoriserede medarbejdere. Disse er udvalgte nøglemedarbejdere; medarbejderne i DRIFT, ledelsesgruppen i IT Center Nord og vagtfirmaet. Ændring af adgang kræver en ledelsesmæssig skriftlig godkendelse, og der foretages gennemgang af eksisterende adgangsrettigheder hvert år og kvitteres i GAK. Øvrige personer med ærinde i serverrummene vil altid være ledsaget af en autoriseret medarbejder.

Adgang til IT Center Nords lokaler sker med personalekort. Der er kun et begrænset antal medarbejdere, ud over IT Center Nords personale, der har adgang.

Organisatoriske sikkerhedsforanstaltninger

It-sikkerhedspolitikken indeholder retningslinjer for oprettelse og nedlæggelse af brugere med systemadministrationsrettigheder, og den enkelte Dataansvarlige er ansvarlig for, at disse retningslinjer overholdes. Dette er især med henblik på, at fratrådte medarbejdere får afleveret deres nøgler og adgangskort, så der ikke længere kan opnås fysisk adgang til bygningerne.

Den enkelte Dataansvarlige er forpligtet til at meddele Databehandleren, når brugere med systemadministrationsrettigheder fratræder. Den enkelte Dataansvarlig er selv ansvarlig for oprettelse og nedlæggelse af egne brugere.

Alle Databehandlerens ansatte følger et awarenes-program, som gennemgår både it sikkerhed og GDPR-relaterede spørgsmål, hver session afsluttes med nogle få spørgsmål, og der følges op på, hvorvidt de enkelte medarbejdere har fuldført sessionerne.

Der er lavet plakater med 10 opmærksomhedspunkter i forhold til GDPR, som hænger forskellige steder i bygningen. Disse har også kørt som logon-skærm.

Dokumentejer, godkender og versionering

Ejer: Claus Larsen

Godkender: Direktør Lisbeth Nørgaard

Dato	Version	Forfatter	Ændringsbeskrivelse
10.06.2021	1.5	BEK	Tilføjet henvisning til ”produktkatalog_sikkerhed” under Vejledninger i tilslutning til denne politik

04.05.2021	1.4	HLO /BEK	Tilføjet henvisning til Databehandler-aftale bilag 2c under afsnittet ”Sikkerhedsforanstaltninger”. Bilag 2c er tilføjet som bilag 1 i IT-sikkerhedspolitikken
22.04.2021	1.3	BEK	Tilføjet ”Procedure for beredskab ved brud på datasikkerheden” under afsnittet ”Vejledninger i tilslutning til denne politik”
15.04.2021	1.2	CLL/BEK	Tilretning af kilder, samt tilretning af afsnit ”Sikkerhed i forbindelse med brug af databehandlere” vedr. opfølgning på dokumentation af it-sikkerheden
12.02.2021	1.1	CLL	Der er foretaget ændringer som følge at SOSU Esbjergs nye samarbejde med IT-Center Nord om drift af IT.
25.08.2018	1.0	CLL	-