Databeskyttelsespolitik for Jordbrugets Uddannelses Center Århus

Revideret nov. 2019

Indholdsfortegnelse

Indhold

Introduktion

Denne databeskyttelsespolitik, som er besluttet af bestyrelsen, udgør den overordnede ramme for at opretholde datasikkerheden på Jordbrugets UddannelsesCenter Århus (JU). Hermed ønsker skolen at demonstrere sin seriøse holdning til at skabe sikkerhed for persondata, systemer og it-aktiver.

Hensigten er at lægge et fundament, så kritiske og fortrolige informationer og systemer kan bevare deres fortrolighed, integritet og tilgængelighed.

Formål

Formålet med denne politik er, at vi på JU sørger for, at oplysninger ikke bliver videregivet til uvedkommende enten bevidst eller uforvarende. Der er derfor i denne politik og de dertilhørende dokumenter formuleret et samlet sæt regler for, hvordan vi på JU håndtere personoplysninger.

Idet brugen af it anses for at være en meget vigtig forudsætning for JU´s eksistens, vil det være nødvendigt at sikre skolens it-ressourcer (data, software, hardware og kommunikationsforbindelser).

Derfor vil vi etablere og vedligeholde en afbalanceret it-sikkerhed, som i denne sammenhæng omfatter alle nødvendige organisatoriske, fysiske og tekniske sikkerhedsforanstaltninger.

It-ressourcerne skal med andre ord beskyttes mod misbrug, manipulation, ødelæggelse og tab, samt mod at blive fejlbehæftede. Beskyttelsen skal virke mod alle former for trusler, interne eller eksterne, hændelige eller bevidste.

Ledelsens udmelding om de overordnede mål og principper

JU ønsker at opnå:

- 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
- Opretholdelse af et image som en skole, der demonstrerer kvalitet og sammenhæng i brugen af it

Databeskyttelsespolitikken skal danne grundlag for at forebygge og begrænse skader til en, for skolen, kendt og accepteret størrelse samt sikre fortsat it-drift efter et sikkerhedsbrud – inden for en nærmere defineret tidshorisont.

Databeskyttelsesrådgiver (DPO)

JU som institution anses som en offentlig virksomhed og skolen har derfor valgt at have tilknyttet en DPO. JU har indgået aftale med Arild Ehrenskjöld, Sønderhøj 9, 2. tv, 8260 Viby J., e-mail ague@efif.dk, telefon: 86363220, om at være skolens databeskyttelsesrådgiver.

Datasikkerhedsudvalg

Der er på JU nedsat et datasikkerhedsudvalget. Datasikkerhedsudvalget er den samlede enhed som forholder sig til alt omkring GDPR (persondataforordningen) og som er ansvarlig for alt arbejdet med persondata på JU. Udvalget består af:

- IT-leder, Henning Randrup hrt@ju.dk tlf.: 61221738
- Administrationschef, Karin Reinholdt, krn@ju.dk tlf.: 61614268
- Tekniskchef, Rasmus Christensen rac@ju.dk tlf.: 24477881
- Uddannelsesleder, Poul Arne Jansen paj@ju.dk tlf.: 20455634
- Direktør, Peter L. Moesgaard plm@ju.dk tlf.: 40417380

Politik for behandling af persondata

JU´s politik for behandling af persondata er beskrevet i dokumenterne ”Persondatapolitik for elever, studerende samt kursister” og ”Persondatapolitik for ansatte samt tilknyttet personale” og der henvises til disse for en nærmere beskrivelse.

Procedure i forbindelse med henvendelser fra registrerede

På JU håndteres alle henvendelser af det administrative personale. I persondatapolitikken, som virksomheder, elever, censorer og ansatte er bekendt med, har vi anført vores kontaktoplysninger for disse henvendelser.

De registreredes vigtigste rettigheder efter databeskyttelsesforordningen er:

- Retten til at modtage oplysning om behandling af deres personoplysninger (oplysningspligt).
- Retten til at få indsigt i deres personoplysninger.
- Retten til at få urigtige personoplysninger rettet.
- Retten til at få deres personoplysninger slettet.
- Retten til at gøre indsigelse mod at personoplysninger anvendes til direkte markedsføring.
- Retten til at gøre indsigelse mod automatiske individuelle afgørelser, herunder profilering.
- Retten til at flytte deres personoplysninger (data-portabilitet).

Alle ovenstående rettigheder håndteres manuelt ved henvendelse som anført i persondatapolitikkerne for henholdsvis elever, studerende og kursister samt ansatte.

Vigtige grundprincipper for sikkerhedsarbejdet

Funktionsadskillelse
Direktøren beslutter hvem, der skal have adgang til hvilke ressourcer og hvornår. Datasikkerhedsudvalget, definerer rettigheder/begrænsninger i overensstemmelse med direktørens beslutninger. Brugere og rettigheder administreres i systemet Perssys. Oprettelse, ændring og sletning af brugere og rettigheder kan kun finde sted efter godkendelse af den pågældende ansattes leder.

Sikkerhedsforanstaltninger
Direktøren beslutter omfang og styrke af de sikkerhedsforanstaltninger, som det findes nødvendigt at installere. Den it-ansvarlige installerer de tekniske foranstaltninger, mens direktøren står for formuleringen af de administrative foranstaltninger (retningslinjer og instrukser).

Styring af sikkerhedshændelser
Vi vil løbende vurdere hændelser, der kan true sikkerheden, så risikobilledet kan opdateres ved gennemgang af såvel kendte som nye trusler og sårbarheder. Samtidig vil vi vurdere om der skal indføres nye tiltag. Direktøren rapporterer overordnet til bestyrelsen om de hændelser, der måtte være sket, og informerer om det opdaterede risikobillede, når væsentlige ændringer er indtruffet.

Sikkerhed i forbindelse med outsourcing
Leverandører, der helt eller delvist står for drift af JU´s 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 outsourcing, skal der udarbejdes en databehandleraftale, der i detaljer beskriver de sikkerhedskrav, som leverandøren skal leve op til. Leverandører skal én gang om året indhente en revisionserklæring fra en uafhængig tredjepart, om, at it-sikkerheden er i orden.

EFIF har udarbejdet 2 skabeloner til databehandleraftaler, én for dataansvarlige og én for databehandlere. Disse skabeloner lægges til grund for databehandleraftaler, hvor leverandøren ikke selv har udarbejdet udkast.

Hovedpunkterne i retningslinjerne for IT-sikkerheden på JU.

1. Overordnede retningslinjer (informationssikkerhedspolitikker)
Vi har brug for et sikkerhedsniveau afstemt efter omkostningerne og de forretningsmæssige behov. Ledelsen har derfor sammenfattet sine overordnede krav i nærværende databeskyttelsespolitik.

2. Organisering af sikkerhedsarbejdet
Som beskrevet tidligere er direktøren ansvarlig for den overordnede it-sikkerhed samt for udformning af nærværende databeskyttelsespolitik. Samtidig er det direktøren, der beslutter hvem, der skal have adgang til hvilke it-ressourcer og hvornår. En udpeget it-ansvarlig definerer rettigheder/begrænsninger i overensstemmelse med disse beslutninger

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

3. Medarbejdersikkerhed
Der skal informeres og stilles krav om it-sikkerheden til medarbejderne før og under ansættelsen samt efter ansættelsens ophør eller ændring. Specielt vil der være særlige sikkerhedskrav forbundet med arbejde i hjemmet eller ved andet arbejde uden for kontoret (på privat it-udstyr eller på firmaejet udstyr). Ved ansættelse udleveres skolens udarbejde dokument ”Sikker behandling af personoplysninger og informationsaktiviteter”, som alle ansætte forudsættes at arbejde efter for at minimere risikoen for brud på datasikkerheden.

4. Styring af aktiver
JU´s it-aktiver (software, data, eller fysiske enheder) skal identificeres og registreres, så det er muligt at definere, hvilke der er kritiske, vigtige eller sensitive for skolen.

Hertil er det nødvendigt at udpege en ejer for hvert aktiv, således at denne har ansvaret for korrekt håndtering af det enkelte aktiv.

Klassifikation skal sikre passende beskyttelse af information, der står i forhold til informationens betydning for organisationen.

I forhold til mediehåndtering skal det forhindres, at uautoriseret offentliggørelse, ændring, fjernelse eller ødelæggelse af information lagret på medier (inkl. papirmediet) finder sted.

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

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

5. Adgangsstyring
Der skal gennemføres styring af den generelle adgang til skolens systemer, informationer og netværk med udgangspunkt i de forretnings- og lovgivningsbetingede krav.

Der skal desuden kunne gennemføres begrænsninger i adgangen til specifikke systemer og data ved at definere brugerroller og ved at tildele privilegerede adgangsrettigheder.

Der skal udarbejdes procedurer for brugerregistrering og -afmelding samt for tildeling af brugeradgang.

System- og dataejere bør med jævne mellemrum gennemgå tildelte rettigheder for at konstatere, om de fortsat er gældende.

Der skal gøres brug af sikre adgangskoder/passwords samt sikkert log-on; begge dele beskrives i retningslinjer for IT-adfærd på JU, der fremgår af skolens dokument: ”Sikker behandling af personoplysninger og informationsaktiviteter.

6. Kryptering
Der skal tages stilling til i hvor høj grad, der skal gøres brug af kryptering af såvel lagrede data som data under transmission.

Behovet for at anvende kryptering baseres på en risikovurdering. Ansvaret for det praktiske arbejde samt for nøgleadministration vil i givet fald blive beskrevet i procedurer.

7. Cloudtjenester
Skolen digitale undervisningsplatform er baseret på Office 365. Platformen indeholder identifikationsoplysninger og undervisningsmaterialer. Det er ikke tilladt at benytte andre cloudtjenester til opbevaring af skolens data.

8. Fysisk sikring og miljøsikring
Kritisk it-udstyr skal være anbragt i sikre områder beskyttet af de nødvendige fysiske barrierer, adgangskontroller samt alarmer for at minimere risikoen for uheld og ulykker. Endvidere skal kritisk udstyr sikres mod forsyningssvigt (blandt andet el-, vand- og teleforbindelser).

9. Driftssikkerhed

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.

Desuden skal der gennemføres en styring af tekniske sårbarheder, for at forhindre, at disse udnyttes i skadeligt øjemed.

10. Kommunikationssikkerhed

JU´s interne netværk skal styres og overvåges samt have installeret passende sikkerhedsforanstaltninger. Forekommer der flere forskellige brugergrupper på netværket, skal dette opdeles, så grupperne af brugere bliver adskilt.

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

Blandt andet kan der blive tale om at etablere særlige aftaler om fortrolighed og hemmeligholdelse samt brug af kryptering, når det drejer sig om data af højeste klassifikation.

11. Anskaffelse, udvikling og vedligeholdelse af systemer

Sikkerhed skal indgå 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 bør ske på basis af en risikovurdering.

Særlige overvejelser skal ske vedrørende brugen af persondata i forbindelse med testforløb.

12. Leverandørforhold

Outsourcing skal være baseret på en kontrakt samt en databehandleraftale, som sikrer, at virksomhedens 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 virksomhedens systemer via eksterne netværk, skal overholde virksomhedens sikkerhedspolitik og –retningslinjer. Dette gælder også medarbejderes brug af private computere, tablets og mobiler, hvis de har opnået tilladelse til opkobling.

13. Styring af brud på informationssikkerhed
Styring af brud på informationssikkerhed betegnes også ”Information Security Incident Management”. Det skal sikre en ensartet og effektiv metode til at styre sikkerhedsbrud – herunder kommunikation om sikkerhedstruende hændelser og svagheder.

Ting, der beskrives, er blandt andet: ansvar og procedurer, hændelsesrapportering, rapportering af svagheder, vurdering af hændelser, håndtering af sikkerhedsbrud, opsamling af erfaring fra sikkerhedsbrud, samt indsamling af beviser (der i givet fald kan bruges i en retslig tvist). Dette er nærmere beskrevet i JU´s ”beredskabsplan for data og IT-brud”

14. Beredskabsstyring m.m.
Beredskabsstyring handler om ”sammenhæng i informationssikkerhed”. Det skal gerne forankres i skolens generelle procedurer for nød-, beredskabs- og reetableringsstyring.

Skolen skal indføre beredskabsstyring som en løbende opgave med det formål at begrænse konsekvenserne ved katastrofer, sikkerhedsbrud og mistet tilgængelighed.

Det indebærer specifikation af krav til beredskab samt af beredskabsplaner. Beredskabsstyringen skal indeholde procedurer, der identificerer og reducerer risici, begrænser konsekvenserne ved skadelige hændelser og sikrer rettidig reetablering af kritiske forretningsprocesser.

En nødplan skal sikre muligheden for hurtigst muligt at reetablere normal drift efter en større katastrofe (brandskade, vandskade, mv.)

For at omgå (mindre) tekniske problemer, kan det overvejes at have ekstra udstyr parat.

15. Overensstemmelse med lovbestemte og kontraktlige krav
Vi vil forhindre, at der sker brud på relevante sikkerhedskrav i henhold til lovgivning, bekendtgørelser, cirkulærer og myndighedsforordninger i øvrigt, samt i indgåede kontraktlige forpligtelser.

Revidering og opfølgning

Datasikkerhedsudvalget sikre en løbende opfølgning og revidering af nærværende samt tilhørende dokumenter. Det er indskrevet i skolens kvalitetspolitik, at der som minimum en gang om året laves en systematisk gennemgang, for at sikre at vi til stadighed lever op til de gældende krav og retningsliner på området.

Øvrige dokumenter

Der henvises til følgende dokumenter som understøtter nærværende databeskyttelsespolitik:

- Persondatapolitik for elever, studerende samt kursister
- Persondatapolitik for ansatte samt tilknyttet personale
- Sikker behandling af personoplysninger og informationsaktiviteter
- Samtykke erklæring for elever, studerende samt kursister
- Diverse fortegnelser