Designskolen Kolding Informationssikkerhedspolitik

(ISO 27001:2013)

Opdateret på baggrund af
Persondataforordningen (GDPR) 25.5.2018.

Indhold

5. Informationssikkerhedspolitikker

5.1. Retningslinjer for styring af informationssikkerhed

5.1.1. Politikker for informationssikkerhed

Designskolen Koldings informationssikkerhedspolitik skal offentliggøres og kommunikeres til alle relevante interessenter, herunder især medarbejdere, studerende og samarbejdspartnere.

Informationssikkerhed defineres som de samlede foranstaltninger til at sikre fortrolighed, tilgængelighed og integritet i overensstemmelse med gældende persondataforordning (GDPR). Foranstaltninger inkluderer tekniske, proceduremæssige, lov- og regelmæssige kontroller.

Informationssikkerhedspolitikken skal godkendes af rektoratet og derefter forelægges Designskolen Koldings bestyrelse.

5.1.2 Gennemgang af politikker for informationssikkerhed

Politikkerne for informationssikkerhed skal årligt gennemgås af informationssikkerhedsgruppen for at sikre deres fortsatte egnethed, tilstrækkelighed og aktualitet.

6. Organisering af informationssikkerhed

Informationssikkerheden på Designskolen Kolding er styret af klare retningslinjer og regler samt en tydelig ansvarsfordeling. Ansvaret er hierarkisk placeret med skolens øverste ledelse, rektoratet, som hovedansvarlig for overholdelse og implementering af informationssikkerhedspolitikken, både internt og i samarbejdet med eksterne partnere.

6.1. Interne organisatoriske forhold

Rektoratet har det øverste ansvar for informationspolitikken og har i denne kapacitet valgt at uddelegere dele af ansvaret til relevante funktioner og udvalg.

6.1.1. Roller og ansvarsområder for informationssikkerhed

Chef for talentoptag, beskæftigelse og faciliteter har som informationssikkerhedskoordinator det overordnede ansvar for informationssikkerhed og rapporterer direkte til rektor.
Studie-, kvalitets- og efteruddannelseschef skal som databeskyttelsesrådgiver (DPO) inddrages i alle spørgsmål om databeskyttelse og har en rådgivende og overvågende funktion om de databeskyttelsesretslige regler, især med fokus på behandlingen af personfølsomme oplysninger herunder især på områder, hvor der er større risiko for uretmæssigheder. DPOen er også kontaktperson for og til Datatilsynet.
Derudover har Designskolen Kolding et antal dataejere, som er registreret i et dataejerdokument, som er et internt bilag til Designskolen Koldings Informationssikkerhedspolitik.
Ansvaret for den daglige drift og sikkerhed er placeret hos systemadministratorerne, der rapporterer til informationssikkerhedskoordinatoren.
Designskolen Koldings samarbejdsudvalg er samtidig skolens informationssikkerhedsudvalg og har ansvar for at sikre, at politikken for informationssikkerhed er synlig, koordineret og i overensstemmelse med Designskolen Koldings strategi.

6.1.2. Funktionsadskillelse

Systemadministratorerne er ansvarlig for den daglige drift.
Informationssikkerhedskoordinatoren foretager jævnlig stikprøvekontrol af overholdelse af procedurer i informationssikkerhedspolitikken.

6.1.3. Kontakt med myndigheder

Systemadministratorerne er ansvarlige for vedligeholdelse af oversigt over de væsentligste kontakter hos relevante myndigheder i relation til informationssikkerhed.
Informationssikkerhedskoordinatoren er ansvarlig for anmeldelser til Datatilsynet, herunder for eventuelle brud på Persondataforordningen indenfor 7 dage efter et sådant brud opdages.

6.1.4. Kontakt med særlige interessegrupper

IT-afdelingen skal gennem abonnement på relevante nyhedsbreve og i samarbejde med relevante leverandører sikre sig adgang til opdateret viden om sikkerhed, risici, beskyttelsesmetoder og -værktøjer. Relevante interessenter skal informeres om informationssikkerhedspolitikken på Designskolen Kolding.

6.1.5. Informationssikkerhed ved projektstyring

I forbindelse med alle projekter, både interne og eksterne, skal organisationens regler og gældende lovgivning for beskyttelse af materiel samt data overholdes af alle involverede medarbejdere.
For Forsknings- og Udviklingsprojekter, se appendix A.

6.2. Mobilt udstyr og fjernarbejdspladser

Skolens medarbejdere benytter sig i vid udstrækning af mobilt udstyr, og informationssikkerhedspolitikken indeholder derfor klare regler for brug af dette.

6.2.1. Politik for mobilt udstyr

Alt mobilt udstyr, herunder computere og telefoner, skal beskyttes med password og/eller Touch ID. Udleveret udstyr er strengt personligt og må kun benyttes af medarbejderen. Medarbejderen hæfter for skader påført udstyret af andre, hvis udstyret har været brugt uden for arbejdsmæssig sammenhæng. Det udleverede maskinel må ikke benyttes som host for servere og bit-torrent-programmer. Mobiltelefoner benyttes i overensstemmelse med abonnement. (Se nærmere regler i Personalehåndbogen). Gældende love og regler forventes overholdt, og ophavsrettigheder forventes respekteret.

6.2.2. Fjernarbejdspladser

Det er ikke muligt at få stillet en egentlig fjernarbejdsplads til rådighed, men udleveret mobilt udstyr må benyttes som sådan via VPN-opkobling ifølge ovenstående politik for mobilt udstyr.

7. Personalesikkerhed

Designskolen Kolding er opmærksom på at gennemføre en kvalitetsmæssig ordentlig og sikker rekruttering og onboarding, herunder at nyansatte medarbejdere kvalificeres til at kunne benytte skolens informationsressourcer inden for de i informationssikkerhedspolitikken angivne principper og regler.

7.1. Før ansættelsen

7.1.1. Screening
Alle ansættelsesudvalg vurderer i forbindelse med ansættelsesforløb, om der skal rekvireres personlige referencer samt straffeattest.

7.1.2. Ansættelsesvilkår og -betingelser
Som en del af ansættelseskontrakten giver medarbejderen tilsagn til, at vedkommendes data må opbevares og behandles efter gældende lovgivning samt accepterer den for skolen til enhver tid gældende Informationssikkerhedspolitik, der beskriver Designskolen Koldings medarbejderes ansvar og forpligtelser vedrørende informationssikkerhed samt regler for brug af det af skolen udleverede materiel. I forbindelse med udlevering af kontrakten udleveres også Designskolen Koldings regler for informationssikkerhed. Det er den ansættende leders ansvar at orientere om, hvorledes data og dokumenter skal klassificeres samt den enkelte afdelings placeringsmuligheder for data.

7.2. Under ansættelsen

7.2.1. Ledelsesansvar
Det er rektoratets ansvar at sikre, at alle medarbejdere er grundigt informeret om kravene til behandling af informationer og materiel, herunder persondataforordningen, således at alle medarbejdere kan overholde den til enhver tid gældende lovgivning.
Efter aftale med rektoratet har dataejer i samråd med ansættende leder ansvaret for tildeling af rettigheder.

7.2.2. Bevidsthed om, uddannelse og træning i informationssikkerhed
IT-afdelingen er ansvarlig for løbende at informere både ledelse og medarbejdere om nye tiltag samt nødvendige ændringer i procedurer.
Alle medarbejdere er ansvarlige for at sætte sig ind i og overholde den til enhver tid gældende lovgivning samt Designskolens Koldings regler om informationssikkerhed.

7.2.3. Sanktioner
Medarbejdere, der bevidst overtræder reglerne for informationssikkerhed, indkaldes til samtale med deres nærmeste leder, der vurderer sagens alvor samt dens eventuelle konsekvenser.
Ved grovere overtrædelser indkaldes til samtale med nærmeste leder samt administrationschefen, der vurderer sagens alvor samt dens eventuelle konsekvenser.

7.2.4. Gennemsigtighed
Medarbejdere giver i forbindelse med tiltrædelsen lov til, at Designskolen Kolding under ansættelsen opbevarer og behandler deres data og informationer. Disse data og informationer opbevares fortroligt og deles kun med offentlige myndigheder efter aftale med medarbejderen, fx i forbindelse med sygdom. Designskolen Kolding deler ikke medarbejderdata med tredjepart.

Alle medarbejdere har til enhver tid ret til at få oplyst, hvilke data institutionen ligger inde med om vedkommende. Disse data vil blive gjort tilgængelige for medarbejderen indenfor 14 dage.

7.3. Ansættelsesforholdets ophør eller ændring

7.3.1. Ansættelsesforholdets ophør og ændring

Det er nærmeste leders ansvar at orientere IT-afdelingen om fratrædelser og afskedigelser, således at IT-afdelingen kan lukke mail-konti, telefonnumre m.v. På sidste arbejdsdag tilbageleverer medarbejderen de udleverede informationsressourcer (computer, mobiltelefon, iPads o.l.).
Ved barsel returneres de udleverede informationsressourcer medmindre anden aftale indgås med nærmeste leder og den IT-systemansvarlige.
I tilfælde af strejke/lockout i forbindelse med overenskomstforhandlinger skal medarbejdere aflevere det udleverede materiel, medmindre andet besluttes af rektoratet.
Efter ansættelsens ophør bliver den fratrådte medarbejders AD-konto deaktiveret, herunder mailkonto, der dog i en måned herefter henviser til ny medarbejder og/eller nærmeste leder i form af autosvar.
Den fratrådte medarbejder har efter ansættelsens ophør ret til at blive glemt, dvs. få alle sine data fjernet fra institutionens arkiver, medmindre dette strider mod anden lovgivning.

8. Styring af aktiver

Designskolen Koldings IT-afdeling har det overordnede ansvar for implementering og håndtering af aktiver i overensstemmelse med de nedenfor beskrevne procedurer.

8.1. Ansvar for aktiver

8.1.1 Fortegnelse over aktiver
Det er IT-afdelingens ansvar, at alle fysiske enheder er registreret med ejer, bruger, serienummer, placering og ibrugtagelsesdato. Designskolen Koldings dataregistre (filer, databaser samt andet personfølsomt materiale) registreres og klassificeres i overensstemmelse med Designskolen Koldings politik for håndtering og sikring af data. Registreringen skal løbende vedligeholdes.

8.1.2. Ejerskab af aktiver
IT-afdelingen har ansvar for, at fysiske aktiver vedligeholdes. Hvert aktiv har en ejer, der er ansvarlig for den løbende opdatering og vedligeholdelse i samråd med IT-afdelingen. IT-afdelingen har ansvar for den overordnede sikkerhed på de anvendte platforme.

8.1.3. Accepteret brug af aktiver
Alt udleveret udstyr, herunder computere og telefoner, skal beskyttes med password og/eller fingeraftryk og/eller ansigtsgenkendelse. Udleveret udstyr er strengt personligt og må kun benyttes af medarbejderen. Medarbejderen hæfter for skader påført udstyret af andre, hvis udstyret har været brugt uden for arbejdsmæssig sammenhæng. Det udleverede maskinel må ikke benyttes som host for servere og bit-torrent-programmer. Gældende love og regler forventes overholdt, og ophavsrettigheder forventes respekteret.

8.1.4. Tilbagelevering af aktiver
På sidste arbejdsdag tilbageleverer medarbejderen de udleverede informationsressourcer (computer, mobiltelefon, iPads o.l.) samtidig med at adgangen til skolens aktiver ophæves.
Al tilbageleveret materiel formateres inden eventuel genudlevering.

8.2. Klassifikation af information

8.2.1 Klassifikation af information
Designskolen Kolding opererer med tre niveauer for klassifikation af informationer:

- Offentlige: Materiale, der frit kan udleveres til både interne og eksterne parter uden at fortrolighedsaftaler kræves.
- Interne: Materiale, der er tilgængeligt for alle internt i organisationen.
- (Person)følsomme og fortrolige: Materiale, der udelukkende er tilgængeligt for en begrænset gruppe personer, for hvem det er relevant.

8.2.2 Mærkning af informationer
Med udgangspunkt i de ovenfor angivne niveauer af klassifikation af information vurderer alle medarbejdere, hvorledes data skal behandles og opbevares, og handler derefter.

8.2.3 Håndtering af aktiver
Medarbejdere med adgang til personfølsomt og fortrolig materiale orienteres om fortrolighed.
Fortrolige materielle aktiver beskyttes i aflåste arkivskabe. Disse er placeret i lokaler, der enten er bemandede eller aflåste.

Fortrolige immaterielle aktiver beskyttes via begrænset adgang.
Fortrolig information må ikke udleveres uden eksisterende aftale med dataejer. Ved udlevering skal gældende lovgivning overholdes.
Fortrolige informationer må ikke efterlades uden opsyn i offentligt tilgængelige rum. Der skal udvises forsigtighed ved omtale af fortrolige informationer i offentlige rum. Al fortroligt materiale skal udskrives som fortroligt print.
Alle medarbejdere er ansvarlige for at beskytte fortroligheden i både egne og kollegaers arbejde – og for at reagere, hvis fortroligheden kompromitteres.

8.3. Mediehåndtering

8.3.1. Styring af bærbare medier
Medier med fortrolige data må ikke efterlades uden opsyn i offentlige rum eller benyttes på andet udstyr end Designskolen Koldings udstyr.
Ellers gælder de almene regler for klassifikation samt de ovenfor nævnte regler for håndtering af aktiver.

8.3.2. Bortskaffelse af medier
IT-afdelingen er ansvarlige for at destruere forældede medier, inden de bortskaffes.

8.3.3. Fysiske medier under transport
Digitale medier med fortrolige og/eller personfølsomme oplysninger krypteres eller passwordbeskyttes inden transport eller afsendelse.
Fysiske medier med fortrolige og/eller personfølsomme oplysninger behandles fortroligt under transport og afsendelse.

9. Adgangsstyring

Adgangen til at udføre handlinger på skolens it-systemer beskyttes af et autorisationssystem. Skolens medarbejdere er medvirkende til beskyttelse af informationsaktiverne gennem korrekt brug af autorisationssystemet.

9.1. Forretningsmæssige krav til adgangsstyring

9.1.1. Politik for adgangsstyring
It-afdelingen har det overordnede ansvar for at etablere og vedligeholde procedurer vedrørende adgangsstyring.
Alle brugere skal have unikt brugernavn og bruger-id.
Ved ansættelse af nye medarbejdere tager ansættende leder og IT-afdelingen stilling til, hvilke systemer der skal gives adgang til. Ved omplacering af medarbejdere skal alle rettigheder for den pågældende medarbejder revurderes.

9.1.2. Adgang til netværk og netværkstjenester
Brugere skal kun have adgang til de netværk og netværkstjenester, de er autoriseret til at benytte. Leder og IT-afdelingen tager løbende stilling til, hvilke adgange, der er relevante for den enkelte medarbejder.
Adgangen til det interne netværk fra andre lokationer end Ågade 10 skal benytte kodeord og krypteret VPN forbindelse.

9.2. Administration af brugeradgang

9.2.1. Brugerregistrering og –afmelding
Ved ansættelse af ny medarbejder har ansættende leder ansvar for at orientere Regnskab og IT-afdelingen om opstartsdato. Herefter tager ansættende leder og IT-afdeling i fællesskab stilling til, hvilke adgange er relevante for den nye medarbejder. Regnskab udarbejder brugernavn i form af initialer, så der ikke sker sammenfald med andre brugere, og videregiver dette til IT-afdelingen.
Ved ophør af ansættelse har ansættende leder ansvar for at orientere Regnskab og IT-afdelingen om slutdato. Medarbejderen orienteres om procedure for aflevering af hardware (se 8.1.4.). IT-afdelingen sikrer, at medarbejderes adgang til aktiver ophører ved ansættelsens udløb.

9.2.2. Tildeling af brugeradgang
Brugere skal kun have adgang til de netværk og netværkstjenester, de er autoriseret til at benytte. Ved ændringer af medarbejderes arbejdsopgaver tager nærmeste leder og IT-afdelingen stilling til, hvilke adgange, der er relevante for den enkelte medarbejder.

9.2.3. Styring af privilegerede adgangsrettigheder
Administrative kodeord skal følge samme minimumsregler som øvrige kodeord og skal ændres, hvis udenforstående får kendskab til disse, herunder systemadministratorer, der forlader firmaet.
IT-afdelingen skal sikre, at brugen af systemer begrænses til et minimum af betroede og autoriserede brugere.

9.2.4. Styring af hemmelig autentifikationsinformation om brugere
Ikke relevant.

9.2.5. Gennemgang af brugeradgangsrettigheder

Brugeradgangsrettigheder gennemgås af systemejere og IT-afdelingen i forbindelse med nyansættelser, ansættelsesophør samt omrokeringer.

9.2.6. Inddragelse eller justering af adgangsrettigheder
Ved ophør af ansættelse har ansættende leder ansvar for at orientere Regnskab og IT-afdelingen om slutdato. Medarbejderen orienteres om procedure for aflevering af hardware. IT-afdelingen sikrer, at medarbejderes adgang til aktiver ophører ved ansættelsens udløb.

9.2.7. Reparation og vedligeholdelse af materiel
I forbindelse med reparation og vedligeholdelse af det af Designskolen Kolding udleverede udstyr, kan medarbejder blive bedt om at oplyse sine adgangsoplysninger. Efter endt reparation og/eller vedligeholdelse vil medarbejderen blive bedt om at ændre sit password.

9.2.8. Deling af adgangsoplysninger
I enkelte tilfælde, fx i forbindelse med sygdom, PA-funktion og lignende, kan det være hensigtsmæssigt for en medarbejder at dele sine adgangsoplysninger med en anden medarbejder. I sådanne tilfælde vil begge medarbejdere være omfattet af de generelt gældende krav til fortrolighed.

9.3. Brugernes ansvar

9.3.1. Brug af hemmelig autentifikationsinformation
Kodeord er strengt personlige og må ikke deles med andre, hverken internt eller eksternt i organisationen. Det er brugerens ansvar at vælge tilstrækkeligt sikre kodeord i adgangskontrolsystemerne, se i øvrigt punkt 9.4.2.
Logning af password i browsere må benyttes, så længe den generelle beskyttelse af computeren med password samt anvendelse af password-beskyttet pauseskærm og/eller fingeraftryk og/eller ansigtsgenkendelse anvendes, og medarbejderen låser computeren, når den ikke er i brug, eller når medarbejderen forlader sin plads.

9.4. Styring af system- og applikationsadgang

9.4.1. Begrænset adgang til informationer
Adgang til systemer og data styres i overensstemmelse med politikken for brugeradgang (se 9.2.).

9.4.2. Procedurer for sikker log-on
Ved brugeroprettelse eller nulstilling af kodeord skal brugere tildeles en sikker, midlertidig adgangskode, som skal ændres umiddelbart efter første anvendelse.
Kodeord skal indeholde kombinationer af store og små bogstaver samt tal og specialtegn.
Kodeord skal være mindst 8 tegn langt.
Der må ikke benyttes brugernavn, navn eller datoer som en del af kodeord.
De 5 seneste kodeord opbevares i Designskolens Koldings login-system og kan ikke genbruges.
Kodeord skal skiftes efter højst 100 dage. 14 dage før passwordet udløber, vil systemet udsende en automatisk reminder, der bliver gensendt 3 gange.
Et eksempel på et avanceret password kunne være: D3$ign§k0l3n (dette password må du ikke bruge – det er blot til inspiration).

9.4.3. System for administration af adgangskoder

Ved ansættelse udleveres engangskode af IT-afdelingen. Ved første login udskiftes denne til en personlig kode, der overholder ovenstående retningslinjer.
Ved ophør af ansættelse deaktiveres alle personlige koder.

9.4.4. Brug af privilegerede systemprogrammer
Der må ikke installeres tredjeparts-programmer, der kan omgå organisationens fastsatte sikkerhedsprocedurer.

9.4.5. Styring af adgang til kildekoder til programmer
Designskolen Kolding egenudvikler ikke programmer med kildekode men benytter godkendte softwarefirmaer som softwareleverandør.

10. Kryptografi

10.1. Kryptografiske kontroller

10.1.1. Politik for anvendelse af kryptografi
Personfølsomme og fortrolige dokumenter må ikke forefindes på individuelle maskiner, men skal opbevares og tilgås på journaliseringssystem via VPN-forbindelse.
Alle data på medarbejderes bærbare computere og mobile enheder skal altid beskyttes med enten password, pinkode, fingeraftryk og/eller ansigtsgenkendelse.
Personfølsomme og fortrolige oplysninger, der sendes via mail, krypteres via Nem-ID Digital Signatur.
Undtaget herfor er mailkorrespondancer med danske respondenter, som ikke kan modtage krypterede mails. Til disse bruges i stedet e-Boks.
Også undtaget herfor er mailkorrespondancer med udenlandske institutioner, hvor der i stedet indgås databehandlingskontrakter, hvis disse skal modtage personfølsomme eller fortrolige data.

10.1.2. Administration af nøgler
Designskolen Kolding anvender ikke krypteringsnøgler.

11. Fysisk sikkerhed og miljøsikring

Fysisk sikkerhed og adgangsregler for gæster er naturlige elementer i skolens sikkerhedspolitik. Fysisk sikkerhed omfatter blandt andet døre, vinduer, alarmer – samt tyverisikring af skolens fysiske aktiver, eksempelvis it-udstyr. Systemer til adgangskontrol er et naturligt element af skolens sikkerhedspolitik og medvirker til at sikre, at kun personer med legalt ærinde får adgang til skolen.

11.1. Sikre områder

11.1.1. Fysisk perimetersikring
Data, herunder følsomme og kritiske, hostes på UC-Syds server, hvorfor de varetager perimetersikringen.
Yderligere følsomme data hostes af STADS, MDC Nordic og HR-Manager, som hver for sig selv står for sikringen af faciliteterne.

11.1.2. Fysisk adgangskontrol
Adgang til teknikrum og hovedkrydsfelter tillades kun af IT-afdelingen og pedel.
Alle krydsfelter og andre teknikrum skal være aflåste.

11.1.3. Sikring af kontorer, lokaler og faciliteter
Alle kontorer aflåses, når de ikke benyttes. Efter arbejdstids ophør er der kun adgang til skolen via personlige medarbejder- samt studiekort. Medarbejder- og studiekort er personlige og skal opbevares forsvarligt. Bygningens indgangsdøre låses automatisk.
Administration af medarbejder- og studiekort samt nøgler til Designskolen Kolding varetages af pedellen.
Designskolen Kolding har videoovervågning på alle ind- og udgange samt udvalgte lokaler. Disse optagelser bruges udelukkende i forhold til opklaring af kriminelle handlinger og opbevares i 30 dage, hvorefter optagelserne slettes automatisk.

11.1.4. Beskyttelse mod eksterne og miljømæssige trusler
Dataopbevaring er udliciteret til UC-Syd, som har ansvaret for sikker og forsvarlig opbevaring, herunder beskyttelse mod diverse trusler.

11.1.5. Arbejde i sikre områder
Ikke relevant.

11.1.6. Områder til af- og pålæsning
Ikke relevant.

11.2. Udstyr

11.2.1. Placering og beskyttelse af udstyr
Udstyr skal placeres eller beskyttes, så risikoen for skader og uautoriseret adgang minimeres. Udstyr der benyttes til at behandle kritiske/følsomme informationer skal placeres, så informationerne ikke kan ses af uvedkommende.
Bærbare enheder skal fjernes fra skolens område eller opbevares i aflåste kontorer efter endt arbejdstid.

11.2.2. Understøttende forsyninger (forsyningssikkerhed)
Dataopbevaring er udliciteret til UC-Syd, som har ansvar for at sikre de understøttende forsyninger.

11.2.3. Sikring af kabler
Alle forsyningskabler til netværk er låst inde.

11.2.4. Vedligeholdelse af udstyr
IT-afdelingen har ansvar for vedligeholdelse af udstyr efter leverandørens anvisning. Kun godkendte leverandører må udføre reparationer og vedligeholdelse. IT-afdelingen er ansvarlig for at registrere alle fejl og mangler samt reparationer i udstyrsdatabasen.

11.2.5. Fjernelse af aktiver
Udleveret personligt udstyr må som udgangspunkt altid medbringes fra skolens område. Andet udstyr, information og software må kun fjernes fra skolens område med tilladelse fra IT-afdelingen. Udlån og fjernelse af disse aktiver registreres i udstyrs-databasen. Udlån skal være tidsbegrænset.

11.2.6. Sikring af udstyr og aktiver uden for organisationen
Alt udstyr er tyverimærket og sikres ved hjælp af password, pinkode, fingeraftryk og /eller ansigtskendelse. Adgang til skolens data uden for skolens område skal foretages via VPN-adgang.

11.2.7. Sikker bortskaffelse eller genbrug af udstyr
Før udstyr bortskaffes eller genbruges, slettes eller destrueres fysiske harddiske. IT-afdelingen er ansvarlig herfor.

11.2.8. Brugerudstyr uden opsyn
IT-afdelingen har ansvaret for, at udstyr i fællesområder er forsvarligt sikret med fysisk sikring.

11.2.9. Politik for ryddeligt skrivebord og blank skærm
Fortrolige dokumenter fjernes fra skriveborde ved arbejdstid ophør. I løbet af arbejdsdagen vendes dokumenter med blank side opad, hvis skrivebordet forlades. Computerskærme låses, når arbejdsstationen forlades.

12. Driftssikkerhed

Designskolen Koldings servere og netværk holdes opdaterede for at sikre det af rektoratet fastsatte ønskede sikkerhedsniveau for skolen.

12.1. Driftsprocedurer og ansvarsområder

IT-afdelingen er ansvarlig for, at alle sikkerhedsregler og procedurer følges i den daglige drift, samt at problemer og fejl opdages, udbedres og rapporteres. IT-afdelingen indgår i det løbende arbejde (forslag og implementering) med forbedrende sikkerhedstiltag (procedurer, metoder, produkter).
IT-driften skal planlægges på en sådan måde, at såvel den daglige som den periodiske drift kan afvikles korrekt og til tiden. Driftsplanen skal udarbejdes i tilpas god tid i samarbejde med relevante brugere.
Der skal forefindes relevant, detaljeret og opdateret teknisk netværksdokumentation for Designskolen Koldings lokalnet og eksterne forbindelser. Dokumentationen skal have en detaljeringsgrad og form, så tredjepart (eksempelvis konsulenter) vil kunne benytte den i en krisesituation.

12.1.2. Ændringsstyring

Der skal foreligge aktuel driftsdokumentation, der beskriver maskin- og systemmiljøet, samt de forskellige driftsopgaver, manuelle og maskinelle.
IT-driften skal løbende kontrolleres med henblik på hurtig afhjælpning af problemer, fejl og forsinkelser. Kontrollen skal så vidt muligt udføres automatisk.
Større service foregår så vidt muligt uden for almindelig arbejdstid (8.00 – 16.00). For særlige systemer kan der efter aftale med systemejer konkret fastsættes alternative serviceperioder, såfremt brugen af systemerne nødvendiggør dette.
Det efterstræbes, at al planlagt nedetid udmeldes så tidligt som muligt, dog mindst 24 timer før. Planlagt nedetid må så vidt muligt ikke forekomme i den almindelig arbejdstid. Undtagelser skal godkendes af administrationschefen.

12.1.3. Kapacitetsstyring

Designskolen Koldings serverdrift styres af UC-Syd. Der henvises derfor ved dette punkt til deres politik for kapacitetsstyring.

12.1.4. Adskillelse af udviklings-, test- og driftsmiljøer

Designskolen Kolding har ikke udviklings- og testmiljø, og dermed er der ikke behov for adskillelse.

12.2. Beskyttelse mod malware

12.2.1. Kontroller mod malware

Alle Designskolen Koldings maskiner er udstyret med virusbeskyttelse, der beskytter mod malware. Herudover forudsættes en passende brugerbevidsthed, der understøttes af informationer om malware/phishing fra IT-afdelingen.

12.3. Backup

12.3.1 Backup af information

Da Designskolen Koldings servere administreres af UC-Syd, er denne institution også ansvarlig for backup af information. Designskolen Koldings IT-afdeling får dagligt mails med backup-log.

12.4. Logning og overvågning

12.4.1. Hændelseslogning
Designskolen Kolding foretager ikke hændelseslogning, men ved hver enkel utilsigtet hændelse foretages en vurdering af, om denne bør forårsage ændringer i procedurer og drift.

12.4.2. Beskyttelse af log-oplysninger

Designskolen Kolding foretager ikke logning.

12.4.3 Administrator- og operatørlog

Designskolen Kolding foretager ikke logning.

12.4.4. Tidssynkronisering

Alle klienter og servere synkroniserer tiden med domæne-kontrolleren.

12.5. Styring af driftssoftware

12.5.1. Softwareinstallation på driftssystemer

IT-afdelingen er ansvarlig for styring og opdatering af softwareinstallation på driftssystemer.

12.6. Sårbarhedsstyring

12.6.1. Styring af tekniske sårbarheder

Designskolen Kolding orienterer sig om tekniske sårbarheder i institutionens informationssystemer og træffer derudfra beslutninger om eventuelle nødvendige foranstaltninger.

12.6.2. Begrænsninger på softwareinstallation

I og med de maskiner Designskolen Kolding stiller til rådighed for medarbejderne, er at betragte udelukkende som arbejdsredskaber, henstilles der til den enkelte medarbejder, at arbejdsrelevante apps/programmer vælges med omhu, samt at der udvises sund skepsis i forbindelse med installation af apps/programmer på udleveret udstyr.

12.7. Overvejelser i forbindelse med audit af informationssystemer

12.7.1. Kontroller i forbindelse med audit af informationssystemer

Designskolen Kolding gennemfører audit af informationssystemer samt verifikation af driftssystemer jævnligt i overensstemmelse med informationssikkerhedspolitikken og på

en sådan måde, at det ikke forstyrrer institutionens kerneopgave samt øvrige drift mere end nødvendigt.

13. Kommunikationssikkerhed

13.1. Styring af netværkssikkerhed

13.1.1. Netværksstyring

Designskolen Koldings IT-afdeling monitorerer løbende switchene for eventuelle fejl.

13.1.2. Sikring af netværkstjenester

Netværksdriften skal løbende kontrolleres, lokalt eller med fjernovervågning, med henblik på hurtig afhjælpning af problemer og fejl.
Internetlinjen monitoreres eksternt af internetlinje-leverandøren.

13.1.3. Opdeling af netværk
Netværket er delt op i fem netværk:

1. Servicenetværk
2. Managementnetværk
3. Administrationsnetværk
4. Pædagogisk netværk
5. Gæstenetværk

Relevante informationstjenester og informationssystemer er tilgængelige på de enkelte netværk.

13.2. Informationsoverførsel

13.2.1. Politikker og procedurer for informationsoverførsel
Personfølsomme og fortrolige data må ikke opbevares eller deles via cloud-baserede storage-tjenester; dog kan det tillades, hvis IT-afdelingen har godkendt en tjeneste som værende safe harbour (data forbliver i EU).
Designskolen Kolding holder sig løbende orienteret om EU-kommissionens vurdering af, hvilke lande, der er henh. sikre og usikre at overføre persondata og personfølsomme data til, og handler derefter.
Designskolen Kolding overfører kun data til databehandlere, ikke til dataansvarlige, og er bevidste om institutionens ansvar i at sikre, at disse data behandles i overensstemmelse med Persondataforordningens principper.
I forbindelse med overførelse af persondata samt personfølsomme data til institutioner i tredjepartslande indgår Designskolen Kolding den af EU-kommissionen forfattede databehandlings-standardkontrakt med disse.

13.2.2. Aftaler om informationsoverførsel
Ved udveksling af personfølsom information overholdes gældende lovgivning, herunder persondataforordningen.
Ved udveksling af fortrolig information overholdes skolens IT-sikkerhedspolitik.
I forbindelse med overførsel af persondata og personfølsomme data med tredjelande indgås den af EU-kommissionen forfattede standardkontrakt med disse.

13.2.3. Elektroniske meddelelser
Personfølsomme og fortrolige informationer deles med andre offentlige instanser med kryptering og signering med digital medarbejdersignatur (NEM-ID).

Undtaget herfor er mailkorrespondancer med danske respondenter, som ikke kan modtage krypterede mails. Til disse bruges i stedet e-Boks.
Også undtaget herfor er mailkorrespondancer med udenlandske institutioner, hvor der i stedet indgås databehandlingskontrakter, hvis disse skal modtage personfølsomme eller fortrolige data.

13.2.4. Fortroligheds- og hemmeligholdelsesaftaler

Designskolen Kolding opererer med tre niveauer for klassifikation af informationer:

- Offentlige: Materiale, der frit kan udleveres til både interne og eksterne parter uden at fortrolighedsaftaler kræves.
- Interne: Materiale, der er tilgængeligt for alle internt i organisationen.
- (Person)følsomme og fortrolige: Materiale, der udelukkende er tilgængeligt for en begrænset gruppe personer, for hvem det er relevant.

Det er rektoratets og ledelsens ansvar at informere medarbejdergruppen om gældende lovgivning, herunder Persondataforordningen, samt skolens informationssikkerhedspolitik.
Det er den enkelte medarbejders ansvar at være opmærksom på, at fortrolige og personfølsomme data ikke deles via ikke-sikre kommunikationsformer.
Der henstilles til generel årvågenhed over, hvad der deles via e-mails, sociale medier m.v.

14. Anskaffelse, udvikling og vedligeholdelse af systemer

14.1. Sikkerhedskrav til informationssystemer

14.1.1. Analyse og specifikation af informationssikkerhedskrav

Det er IT-afdelingens ansvar at opdatere interne systemer, der ikke længere supporteres af hardware- og softwareudbydere. Samtidig skal IT-afdelingen holde sig konstant opdaterede om udviklingen, så de er informerede om evt. sikkerhedsproblematikker.
Nye serverinstallationer bør så vidt mulig køre på nyest mulige software (serverprogrammel).

14.1.2. Sikring af applikationstjenester på offentlige netværk

Der henstilles til den enkelte medarbejder, at apps/programmer vælges med omhu, samt at der udvises sund skepsis i forbindelse med installation af sådanne apps/programmer på udleveret udstyr.
Ved opståede fejl vil IT-afdelingen være behjælpelige med at føre det udleverede udstyr tilbage til standardinstallation.
Ved mistænkelige hændelser rettes henvendelse til IT-afdelingen.

14.1.3. Beskyttelse af handelsapplikationer og –tjenester

For at beskytte informationer i forbindelse med overførsler af handelsapplikationer og –tjenester er al tilgang til digitale butikker beskyttet af personlig kode og/eller fingeraftryk og/eller ansigtsgenkendelse.

14.2. Sikkerhed i udviklings- og hjælpeprocesser

Designskolen Kolding udvikler ikke selv software og systemer og anvender kun standardiseret software.

14.3. Testdata

Designskolen Kolding udvikler ikke selv software og systemer og anvender kun standardiseret software.

15. Leverandørforhold

15.1. Informationssikkerhed i leverandørforhold

15.1.1. Informationssikkerhedspolitik for leverandørforhold

Ved indgåelse af aftaler med eksterne leverandører specificeres i samarbejdskontrakten, hvilke data m.v. leverandøren har adgang til, samt at leverandøren forpligter sig til at overholde persondataforordningen ved behandling, opbevaring og eventuel videregivelse af disse data. Relevante forhold vedrørende personfølsomme og/eller fortrolige oplysninger samt forhold omfattet af tavshedspligt skal fremgå af kontrakterne med eksterne samarbejdspartnere.
Kravene til informationssikkerhed og behandling af personfølsomme data beskrives således i de kontrakter, der indgås med de eksterne samarbejdspartnere.

Designskolen Koldings netværksleverandører skal i henhold til det aftalte kunne levere:

- De nødvendige teknologiske muligheder for autentifikation og kryptering
- De nødvendige tekniske opsætninger til at sikre opkoblinger i overensstemmelse med samarbejdsaftalen
- Adgangskontrol der sikrer mod uvedkommendes adgang
- Overholdelse af Designskolen Koldings til enhver tid gældende Informationssikkerhedspolitik samt lovgivning, herunder Persondataforordningen.

15.2. Styring af leverandørydelser

Givet Designskolen Koldings størrelse er der kun et begrænset antal leverandører tilknyttet. Disse er Designskolen Koldings IT-afdeling i jævnlig kontakt med, og der er således en konstant tæt opfølgning på, at leverandørerne leverer, hvad de skal og overholder aftalerne.
Herudover involveres Designskolen Koldings DPO i kravsspecifikationerne til leverandørerne.

16. Styring af informationssikkerhedsbrud

16.1.1 Styring af informationssikkerhedsbrud og forbedringer

Ved konstatering af brud eller formodede brud på it-sikringsforanstaltninger – herunder ukendte e-mails, e-mails med ejendommelige overskrifter og fejlbehæftet sprog, dobbelt sign-on hjemmesider, snydetelefonopkald – samt alt andet, der virker påfaldende skal rapportering straks ske til it-afdelingen, som herefter vurderer informationssikkerhedsbruddets grovhed. Dette gælder både for interne medarbejdere og eksterne leverandører.

I tilfælde af alvorlige informationssikkerhedsbrud afrapporterer IT-afdelingen omgående til informationssikkerhedskoordinatoren, der herefter tager stilling til, om bruddet er så alvorligt, at rektoratet skal inddrages.

Brud på sikkerheden, uautoriseret adgang og forsøg på uautoriseret adgang til systemer, informationer og data skal registreres. Hvis et sikkerhedsbrud afstedkommer et retsligt efterspil uanset om sikkerhedsbruddet er foretaget af en person eller en virksomhed, så skal der indsamles, opbevares og præsenteres et fyldestgørende bevismateriale.

Når en sag vedrørende informationssikkerhedsbrud er afsluttet, foretager IT-afdelingen foranstaltninger, der så vidt muligt sikrer, at et tilsvarende brud ikke sker en anden gang.

16.1.2. Styring af persondatasikkerhedsbrud og forbedringer

Hvis en medarbejder konstaterer et brud på persondatasikkerheden, kontaktes dataejer og/eller nærmeste leder. Dataejer tager herefter i samråd med DPOen stilling til bruddets alvor, herunder om dette kan indebære en risiko for fysiske personers rettigheder eller frihedsrettigheder.
IT-afdelingen kan være behjælpelig med vejledning om dette.

Hvis et brud indebærer en risiko, skal den dataansvarlige uden unødvendig forsinkelse og om muligt senest 72 timer efter at denne er blevet bekendt med bruddet, anmelde dette til Datatilsynet.

DPOen skal inddrages af den dataansvarlige i tilfælde af, at konkrete klagesager indbringes for Datatilsynet.

Ved alvorlige og/eller forsætlige brud på persondatasikkerheden orienterer dataejer og nærmeste leder rektoratet, som tager stilling til eventuelle konsekvenser, herunder forbedring af systemer, så sådanne brud ikke gentages.

Når en sag vedrørende persondatasikkerhedsbrud er afsluttet, foretager dataejer foranstaltninger, der så vidt muligt sikrer, at et tilsvarende brud ikke sker en anden gang.

17. Informationssikkerhedsaspekter ved nød-, beredskabs- og reetableringsstyring

Designskolen Kolding har udliciteret opbevaring af data m.v. til UC-Syd. Serverrum og sikring af dette er således omfattet af UC-Syds informationssikkerhedspolitik og beredskab, som Designskolen Kolding er bekendt med.
Elektronisk post opbevares i Microsofts cloud-baserede posttjeneste, som er indbefattet i Safe Harbour-ordningen. Dertil kommer, at visse data vedrørende de studerende opbevares hos STADS, samt at Designskolen Koldings bogholderi benytter økonomistyringssystemet Navision, hvori data derfor også opbevares.
Internt opbevares alt personfølsomme og fortrolige data i et dokumenthåndteringssystem (ESDH).

Designskolen Koldings IT-afdeling er ansvarlig for at vedligeholde og ajourføre en systemejer-oversigt. Systemejerne er ansvarlige for at identificere kritiske processer.

IT-afdelingen er ansvarlig for at udarbejde og vedligeholde en samlet beredskabsplan i tilfælde af nedbrud på et eller flere systemer, hvori det er klart defineret, hvem der har ansvaret for aktivering af beredskabsplaner. Alle medarbejdere skal være informeret om beredskabsplanernes eksistens, og de medarbejdere, der indgår i beredskabsplaner, skal være informeret om dette.

17.2. Redundans

Sikring af data foretages af UC-Syd og er beskrevet i deres informationssikkerhedspolitik. IT-linjer mellem Designskolen Kolding og UC-Syd er af økonomiske årsager ikke redundante, men de fleste af Designskolen Koldings funktioner vil kunne foretages af medarbejderne fra eksterne internetforbindelser.

18. Overensstemmelse

18.1. Overensstemmelse med lov- og kontraktkrav

18.1.1. Identifikation af gældende lovgivning og kontraktkrav

Ledelsen er ansvarlig for at identificere lovgivning, der er relevant for Designskolen Koldings drift, eller udpege en person der er ansvarlig for denne opgave. Ledelsen er ansvarlig for at alle eksterne sikkerhedskrav og Designskolen Koldings håndtering heraf, klarlægges, dokumenteres og løbende vedligeholdes.

18.1.2. Immaterielle rettigheder

Ledelsen har det overordnede ansvar for, at Designskolen Kolding fastholder en nødvendig opmærksomhed på ikke at krænke tredje parts ophavsrettigheder.
IT-afdelingen skal vedligeholde dokumentation for ejendomsretten af licenser.

IT-afdelingen skal løbende kontrollere, at software-licensaftaler overholdes, f.eks. at eventuelle begrænsninger i antal brugere, servere eller kopier overholdes.
IT-afdelingen skal løbende kontrollere, at der kun er installeret autoriserede systemer med autoriserede licenser på materiel udleveret af Designskolen Kolding.
Registrering af software licenser sker gennem it-afdelingen. Det er IT-afdelingens overordnede ansvar, at der er et tilstrækkeligt antal licenser.
Medarbejdere må ikke forpligte Designskolen Kolding ved at acceptere licensvilkår i software, som ikke er forhåndsgodkendt af IT-afdelingen.

Ansatte må ikke kopiere, konvertere eller udtrække information fra billed- og lydfiler eller tilsvarende ressourcer, med mindre dette specifikt tillades fra rettighedshaveren.
Ansatte må ikke kopiere bøger, artikler, rapporter eller andre dokumenter, helt eller delvist, med mindre dette specifikt tillades fra rettighedshaveren. Jf. Copydans regler.

18.1.3. Beskyttelse af registreringer
Ikke relevant

18.1.4. Privatlivets fred og beskyttelse af personoplysninger
I alle sammenhænge, herunder både i forhold til skolens kerneopgave som uddannelsesinstitution samt intern og ekstern kommunikation, bestræber Designskolen Kolding sig på at respektere privatlivets fred samt overholde den til enhver tid gældende lovgivning, herunder Persondataforordningen.

Hvis en medarbejder konstaterer et brud på persondatasikkerheden, kontaktes dataejer og/eller nærmeste leder. Dataejer tager herefter stilling til bruddets alvor, herunder om dette kan indebære en risiko for fysiske personers rettigheder eller frihedsrettigheder.
IT-afdelingen kan være behjælpelig med vejledning om dette.

Hvis et brud indebærer en risiko, skal den dataansvarlige uden unødvendig forsinkelse og om muligt senest 72 timer efter at denne er blevet bekendt med bruddet, anmelde dette til Datatilsynet.

Ved alvorlige og/eller forsætlige brud på persondatasikkerheden orienterer dataejer og nærmeste leder rektoratet, som tager stilling til eventuelle konsekvenser, herunder forbedring af systemer, så sådanne brud ikke gentages.

Når en sag vedrørende persondatasikkerhedsbrud er afsluttet, foretager dataejer foranstaltninger, der så vidt muligt sikrer, at et tilsvarende brud ikke sker en anden gang.

Personoplysninger af fortrolig karakter må kun behandles på mobilt udstyr, hvis dette er password-beskyttet og/eller beskyttet med fingeraftryk og/eller ansigtsgenkendelse, eller disse oplysninger tilgås via VPN-forbindelse.

Ledelsen skal sikre, at medarbejdere informeres om eventuelle overvågningsmuligheder, som Designskolen Kolding kan tage i brug, herunder netværksovervågning ved mistanke om misbrug.

18.1.5. Regulering af kryptografi
Designskolen Kolding skal efterleve de nationale regler for kryptografering. Designskolen Kolding krypterer post, der sendes til styrelser og andre myndigheder via NemID.
Undtaget herfor er mailkorrespondancer med danske respondenter, som ikke kan modtage krypterede mails. Til disse bruges i stedet e-Boks.
Også undtaget herfor er mailkorrespondancer med udenlandske institutioner, hvor der i stedet indgås databehandlingskontrakter, hvis disse skal modtage personfølsomme eller fortrolige data.

Ledelsen og den informationssikkerhedsansvarlige er ansvarlige for at informere medarbejdere om de regler og retningslinjer, der er gældende vedr. udveksling af personfølsomme data.

18.2. Gennemgang af informationssikkerhed

18.2.1. Uafhængig gennemgang af informationssikkerhed
Som netværksudbyder er UC-Syd ansvarlig for sikkerhedsniveauet i interne og eksterne netværksudstyr og servere.

Det er ikke tilladt at forsøge at omgå sikkerhedsmekanismer.
Det er ikke tilladt at foretage uautoriseret afprøvning af sikkerheden.

Bevidste eller gentagne overtrædelser kan medføre, at ansættelses- eller samarbejdsforholdet overvejes fra Designskolen Koldings side.
Hændelser, hvor medarbejdere er involverede, bliver håndteret i overensstemmelse med gældende personalepolitik.
Det er Rektoratets ansvar, at sanktioner for brud på Designskolen Koldings politikker, regler eller retningslinjer håndhæves i overensstemmelse med gældende lovgivning.

18.2.2. Overensstemmelse med sikkerhedspolitikker og sikkerhedsstandarder
Rektoratet skal regelmæssigt sikre, om informationsbehandlingen og -procedurerne inden for IT-området er i overensstemmelse med relevante sikkerhedspolitikker, standarder og andre sikkerhedskrav.

18.2.3. Undersøgelse af teknisk overensstemmelse
IT-afdelingen er ansvarlig for at sikre regelmæssige undersøgelser af, at skolens forskellige systemer er i overensstemmelse med Designskolen Koldings informationssikkerhedspolitikker og –standarder.