Informationssikkerhedspolitik

Marselisborg Gymnasiun

Version: 0.8

April 2018

Indholdsfortegnelse

1.1 Indledning:

Denne informationssikkerhedspolitik er det overordnede rammeværktøj for skolens informationssikkerhed. Politikken tager udgangspunkt i ISO 27001:2013 og afspejler dermed de områder, som er identificeret ved udarbejdelsen af skolens SoA-dokument.

Formålet med informationssikkerhedspolitikken er at tilkendegive overfor alle der har relation til skolen, at anvendelsen og behandling af information og persondata er underkastet retningslinjer. Politikken skal sikre at skolens kritiske informationer om elever, medarbejdere og diverse samarbejdspartnere bevarer deres fortrolighed, integritet og tilgængelighed.

1.2 Omfang og ansvar:

Informationssikkerhedspolitikken omfatter alle kritiske informationer, som skolen er i besiddelse af, uanset hvordan disse opbevares og formidles.
Kritiske informationer defineres som alle persondata, der vedrører medarbejdere, elever, elevers pårørende, eventuelle samarbejdsparter, herunder vikarer, leverandører mv, samt informationer der ikke skal komme til uvedkommendes kendskab.

Informationssikkerhedspolitikken gælder uden undtagelse for alle skolens medarbejdere, herunder fast- og deltidsansatte, som udfører arbejde for skolen, både inden- og uden for skolens matrikler.

1.3 Sikkerhedsniveau:

Skolen fastsætter et sikkerhedsniveau ud fra en risikovurdering, som tager udgangspunkt i kritikaliteten af information og data. Der laves årligt en risikovurdering, som udarbejdes sammen med en konsekvensvurdering under hensynstagen til økonomiske forhold.

Skolen skal altid stile mod at beskytte kritisk data og udelukkende tillade brug af data til medarbejdere med et arbejdsbetinget behov. Adgang og offentliggørelse af informationer, må kun ske i henhold til interne retningslinjer og gældende lovgivning.

Skolen skal udnævne en medarbejder (ansat af skolen), der har det daglige ansvar med at opretholde informationssikkerhedsniveauet. Medarbejderen skal kontrollere, at interne retningslinjer opretholdes og efterleves. I tilfælde hvor informationssikkerheden ikke opretholdes, er det den udpegede medarbejders ansvar, at implementere yderligere foranstaltninger for at opretholde informations-sikkerheden.

1.4 Sikkerhedsbevidsthed:

Informationssikkerhedspolitikken skal kommunikeres ud til alle medarbejdere på skolen for at sikre, at alle er bekendte med retningslinjerne og niveauet af sikkerhed der skal tænkes ind i medarbejdernes daglige arbejde. Alle skolens medarbejdere har selv pligt til at holde sig informeret om retningslinjerne i informationssikkerhedspolitikken.

For at sikre forankring af informationssikkerhedspolitikken hos alle medarbejdere, bør skolens ledelse årligt initiere informationskampagner, for at øge medarbejdernes opmærksomhed på informationssikkerhed.

1.5 Brud på informationssikkerheden:

I det tilfælde hvor en medarbejder bliver bevidst om trusler mod eller decideret brud på informationssikkerheden, skal dette straks rapporteres til relevante instanser. Der skal forelægge en procedure som beskriver processerne omkring hændelseshåndteringen. Denne skal være tilgængelig og kendt af alle medarbejdere, således at informationssikkerhedsbrud bliver håndteret betryggende, og i henhold til skolens forretningsgang på området.

1.6 Dispensation fra informationssikkerhedspolitikken:

Dispensation fra informationssikkerhedspolitikken kan kun ske efter skriftlig tilladelse fra skolens ledelse. Anmodning om dispensationer skal ske på baggrund af en risikovurdering og eventuelt med forslag til kompenserende tiltag.

1.7 Revision af politikker:

Informationssikkerhedspolitikken skal som minimum revurderes årligt samt i forbindelse med større organisatoriske eller teknologiske ændringer. Politikken skal godkendes af skolens bestyrelse på baggrund af en opdateret risikovurdering.

Øvrige politikker og beredskabsplan skal ligeledes revurderes minimum en gang årligt, eller ved betydelige ændringer i det generelle trusselsbillede.

1.8 Beredskab:

Der skal udarbejdes og vedligeholdes en beredskabsplan, som omfatter alle sandsynlige senarier, der kan medføre brud på fortroligheden eller tab af kritisk data. Beredskabsplanen skal indeholde alle

identificerede udefrakommende-, såvel som utilsigtede trusler, som er identificeret og noteret risikovurderingen.
Beredskabsplanen bør løbende opdateres med nuværende trusselsbillede og efterprøves minimum en gang årligt og i henhold til skolens forretningsgang på området.

1.9 A.5 Informationssikkerhedspolitikker

Hensigten med informationssikkerhedspolitikken er at oplyse alle medarbejdere og relevante parter, som arbejder for eller på skolen, omkring de generelle retningslinjer for anvendelse af information og data.
Informationssikkerhedspolitikken skal udleveres til alle medarbejdere i forbindelse med ansættelse.
Nyeste version af politikken skal være tilgængelig for skolens medarbejdere på intranettet.
I stil med skolens egne medarbejdere, skal alle eksterne samarbejdsparter ligeledes gøres bekendt med politikken og efterleve retningslinjer heri.
Informationssikkerheden skal opdateres årligt på baggrund af den aktuelle risikovurdering. Hvis der foretages større organisatoriske eller teknologiske ændringer på skolen, bør der tages stilling til om Informationssikkerhedspolitikken bør revurderes.

1.10 A.6 Organisering af informationssikkerhed

Skolens ledelse har det strategiske ansvar for informationssikkerheden, samt koordinationen heraf på skolen. Der bør af skolens daglige ledelse udpeges en daglig ansvarlig for, at informationssikkerheden bliver opretholdt på et operationelt niveau.

Roller og adgange til systemer bør begrænses og kun tildeles til medarbejdere, der har et arbejdsbetinget behov. Der bør udarbejdes oversigter over hvilke rettigheder der ikke er hensigtsmæssige at enkelte medarbejdere er i besiddelse af. Funktionsadskillelse skal så vidt muligt implementeres i alle relevante led af skolens administrative lag, i det omfang det nu er muligt.

I tilfælde af brud på informationssikkerheden skal medarbejderne være bekendte med de rette kommunikationsveje, herunder rapporteringstidsfrister som måtte eksistere. Alle medarbejdere på skolen bærer et fælles ansvar for at kontakte relevante myndigheder, hvis der opdages et brud på informationssikkerhed.
For at medarbejderne kan løfte rapporteringsansvaret ved sikkerhedsbrud, er det ledelsen på skolens ansvar at sikre kendskab til retningslinjerne for hændelseshåndtering.

1.11 A.7 Personalesikkerhed

Skolens daglige ledelse er ansvarlig for at der bliver udført screening af potentielle nye medarbejdere, inden der indgås et ansættelsesforhold. Screeningen kan eksempelvis indeholde indhentelse af referencer, curriculum vitae og identitetskontrol mv.

Det er skolens daglige ledelses ansvar, at medarbejderne, interne som eksterne, kun er tildelt rettigheder til systemer og data, som afspejler et arbejdsbetinget behov. For at opretholde informationssikkerheden, skal der løbende og i relevant omfang initieres kampagner, som højner medarbejdernes opmærksomhed på informationssikkerheden og forstå vigtigheden heri.

I tilfælde af medarbejders fratrædelse, skal der etableres procedurer, som sikre en ensartet behandling. Dette skal sikre at alle fratrådte medarbejdere får returneret alle udleverede aktiver, herunder Pc'er, nøgler og anden materiel, som måtte være stillet til rådighed af skolen, ITS eller øvrige 3. parter som skolen anvender.
Umiddelbart efter fratrædelse, skal rettigheder og adgange til alle systemer, data og kritiske lokationer inddrages.

1.12 A.8 Styring af aktiver

Det er skolens daglige ledelses ansvar at skolen opretholder og løbende opdaterer fortegnelser over skolens aktiver. Alle aktiver skal tildeles en ejer, som har det overordnede ansvar for aktivet. Alle aktiver udleveret til medarbejdere, bør primært anvendes i arbejdsmæssige sammenhæng.
Alle medarbejdere, vikarer, leverandører mv. skal ved fratrædelse/kontraktens ophør tilbagelevere alle aktiver, som er udleveret af skolen eller ITS.

Information skal klassificeres, således at al information kan inddeles i kategorier, alt efter hvor følsomme informationerne er.
Klassifikationen af data og informationer bør inddeles i fire kategorier:

Offentligt: Data og informationer, som frit kan udleveres til eksterne parter.
Internt brug: Data og informationer, som kun skal benyttes internt blandt skolens medarbejdere. Der kan være tale om mødereferater, fakturaer mv.
Personhenførbare data: Data og information, som er omfattet af Persondataforordningen. Disse skal beskyttes og må kun kendes og behandles af personer, som har et arbejdsbetinget behov for at have kendskab til informationerne. Der bør overvejes kryptering til lagring af data, eller i det mindste opsætte betryggende sikkerhedsforanstaltninger. Der kan være tale om religiøs overbevisning,

helbredsmæssige oplysninger, sociale problemstillinger eller generelle personoplysninger, som kan bruges til at identificere en person eller en snæver personkreds.
Fortroligt: Data og informationer som kun er tilgængelige for en betroet gruppe medarbejdere, som har et arbejdsbetinget behov for at have kendskab til informationerne. Fortrolige informationer må aldrig behandles og lagres på privat udstyr og kræver ekstra høj beskyttelse. Der bør overvejes kryptering til lagring af data, eller i det mindste opsætte betryggende sikkerhedsforanstaltninger.

Data og informationer skal som hovedregel ikke lagres andre steder end på udstyr, som er leveret af skolen eller ITS. Opbevaring af data og informationer på bærbare databærende medier bør begrænses og kun anvendes ud fra et arbejdsbetinget behov.
Ved afskaffelse af databærende medier, herunder Pc'er, servere og harddiske eller lign. skal data og informationer slettes således at disse ikke kan genskabes.

1.13 A.9 Adgangsstyring

Adgangen til skolens systermer og lokationer skal tildeles ud fra et arbejdsbetinget behov.
Adgangen til systemer skal ske igennem unikke brugerprofiler og passwords, og der skal kun gives adgang til et absolut minimum af informationer, data og funktioner i systemerne, som er krævet for at medarbejderen kan udføre sine daglige arbejdsopgaver.
Tildelingen af administrative rettigheder til skolens systemer og netværk, bør kun tildeles et begrænset antal medarbejdere, som alle har et arbejdsbetinget behov for adgangen.
Skolens daglige ledelse skal sørge for at der minimum årligt initieres en gennemgang af tildelte brugerrettigheder, således at de løbende kontrolleres, at medarbejderne kun har de adgangsrettigheder, som det kræves for at udføre deres daglige arbejdsopgaver.

Adgangen til skolens interne netværk, bør som hovedregel kun gives til skolens medarbejdere.
Eleverne bør kun tildeles adgang til et netværket, som er segmenteret fra det netværk, som skolens medarbejdere tilgår.

1.14 A.10 Kryptografi

Data og informationer som enten klassificeres som personfølsomme eller fortrolige, og som overføres til tredjepart skal krypteres således, at de ikke kan blive kendt af uvedkommende.
Krypteringsnøgler skal opbevares forsvarligt og kun være kendte af betroede medarbejdere og samarbejdsparter.
Skolens systemer, der tilbydes og driftes af ITS, har skolen ikke det primære ansvar for.

ITS skal definere en forretningsgang for niveauet for kryptering for systemer og applikationer som ITS varetager.
Skolen er dog fortsat ansvarlige for mobile enheder, PC'er og MAC's der ikke er registeret og indkøbt igennem ITS.

1.15 A.11 Fysisk sikring og miljøsikring

Som hovedregel skal der være etableret tilstrækkelig fysisk perimetersikkerhed for de lokationer, som indeholder personfølsomme eller fortrolige informationer og data. Adgangen til disse lokationer skal tildeles efter et arbejdsbetinget behov.

Servere, krydsfelter og andre tekniske installationer, som måttes findes inden for skolens perimetre, skal placeres således at adgangen hertil kun er tildelt et begrænset antal personer med et arbejdsbetinget behov. Lokalerne hvor sådanne installationer opbevares, skal være indrettet så udefrakommende og miljømæssige trusler minimeres.
Skolens systemer, der tilbydes og driftes af ITS, har skolen ikke det primære ansvar for, da disse varetages og driftes af ITS.
ITS skal definere en forretningsgang for niveauet for fysisk sikring for lokationer som ITS varetager.
Skolen er dog fortsat ansvarlige for deres egen perimetersikkerhed, herunder krydsfelter og servere mv., som fysik er placeret på skolen.

1.16 A.12 Driftsikkerhed

Der skal forelægge driftsprocedurer for alle de systemer og platforme, som ikke er driftet eller leveret af ITS. Driftsprocedurerne skal indeholde retningslinjer for hvordan der skal foretages ændringer til systemerne, hvordan der skal foretages kapacitetsstyrring og hvordan testmiljøer skal være adskilt fra produktionsmiljøer.
For de systemer og platforme, som skolen selv drifter, skal der etableres procedurer og retningslinjer for beskyttelse mod malware, hvordan backup er håndteret, samt hvordan logning og overvågning af miljøerne skal være opsat.
For systemer og platforme der er outsourcet til eksterne leverandører, bør skolerne årligt indhente uvildig revisionserklæring. Denne bør håndteres jævnført skolens retningslinjer omhandlende leverandørstyring.

1.17 A.13 Kommunikationssikkerhed

Der skal på skolens netværk skal være segmenteret, således at elever og skolens medarbejdere ikke benytter samme netværk. Adgangen til skolens administrative netværk, skal kun tildeles efter et

arbejdsbetinget behov og gør som hovedregel ikke tildeles til personer, som ikke er ansat af enten skolen eller ITS.

Ved udveksling af elektroniske meddelelser skal medarbejderen udvise forsigtighed med hvilke informationer der bliver delt og hvordan meddelelserne sendes. Der skal fra skolens ledelse udstikkes klare retningslinjer for hvordan der kommunikeres på en sikker måde, når der skal udveksles persondata og anden fortrolig information.

1.18 A.14 Anskaffelse, udvikling og vedligeholdelse af systemer

Ved indkøb af nye systemer og platforme, hvor indkøbet ikke foregår i samarbejde med ITS, skal systemerne og platformene godkendes og sikres at disse overholder retningslinjerne i informationssikkerhedspolitikken.

1.19 A.15 Leverandørforhold

Det er skolens daglige ledelses på skolens ansvar at der er udarbejdet en politik for leverandørforhold. Indgåelse af leverandøraftaler skal altid indgås på baggrund af en risikovurdering. Ved indgåelse af leverandøraftaler, hvor der er en chance for at leverandøren kommer i kontakt med internt data, personhenførbare data eller fortrolige data, skal der indgås tavshedserklæringer med leverandøren.

Der bør løbende følges op på indgåede leverandøraftaler, for at kontrollere at leverandørerne overholder de ydelser som er aftalt. Ved ændringer til eksisterende leverandørydelser bør leverancen genovervejes for at sikre at ændringen ikke påvirker den oprindeligt udarbejdede risikovurdering. Præcisering af kravene til leverandørstyrring er specificeret i *Retningslinjer for leverandørstyring*.

1.20 A.16 Styring af informationssikkerhedsbrud

Det er skolens daglige ledelses ansvar at der er udarbejdet en politik for håndtering af sikkerhedshændelser. Alle medarbejdere har pligt til hurtigst muligt at rapportere brud på informationssikkerheden. Alle medarbejdere har i deres daglige arbejde ligeledes pligt til at indrapportere observerede svagheder i de benyttede systemer og arbejdsgange.

Ved indrapporterede sikkerhedsbrud skal skolens ledelse vurdere kritikaliteten og om der er tale om tab af tilgængelighed, integritet og fortroligheden af personhenførbar data og fortroligt data. På baggrund af denne vurdering skal relevante handlinger foretages og til en hver tid gældende lovgivning følges med henblik på indrapporteringspligt.

Efter et sikkerhedsbrud skal der indsamles og sikres beviser, så der på baggrund af disse kan konkluderes hvordan bruddet opstod og lignende hændelser kan undgås fremadrettet.

1.21 A.17 Informationssikkerhedsaspekter ved nød-, beredskab- og reetableringsstyring

For alle systemer og platforme, som skolerne har placeret inden for skolens perimetre, skal der være udarbejdet en beredskabsplan, som skal sikre informationssikkerhedskontinuiteten. Systemer som skolen selv har indkøbt og til dagligt selv drifter skal være dækket af denne beredskabsplan.
Niveauet af redundans på disse systemer, skal fastsættes ud fra økonomiske forhold, samt en risikovurdering.
Den udarbejdede beredskabsplan skal opdateres løbende, med de trusler som løbende bliver identificeret. Derudover bør planen afprøves årligt, minimum som en skrivebordsøvelse.

1.22 A.18 Overensstemmelse

Skolens ledelse skal løbende og mindst årligt gennemgå arbejdsgange og processer for at kontrollere at disse er i overensstemmelse med interne politikker og procedurer.

Der skal etableres processer der løbende kontrollerer om al, til en hver tid gældende relevant lovgivning og kontraktuelle krav bliver overholdt i skolens daglige arbejde.

Version	Dato	Forfatter	Kommentar