Danske Gymnasier
Ny Vestergade 13, st.
1471 København K

mail@danskegymnasier.dk
+45 33 18 82 60
danskegymnasier.dk

DANSKE GYMNASIER

29. oktober 2024

Børne- og Undervisningsministeriet
Att. Steen Larsen

Høring vedr. udkast til bekendtgørelse om krav til studieadministrative it-systemer for almene voksenuddannelser, erhvervsuddannelser, arbejdsmarkedsuddannelser, de gymnasiale uddannelser, forberedende grunduddannelse m.fl. (Systemrevisionsbekendtgørelsen).

Danske Gymnasier har den 1. oktober 2024 modtaget høring over udkast til systemrevisionsbekendtgørelse.

Danske gymnasier har ikke nogen kommentarer til de foreslåede ændringer i bekendtgørelsen.

Foreningen vil gerne foreslå en ændring til en af de kontroller, som er en del af systemrevisionen af de studieadministrative systemer. Det omhandler kontrol nr. 20, som vedrører systemleverandørens overholdelse af Databeskyttelsesforordningen. Herunder at der foreligger dokumentation m.m. for behandlingen af personoplysninger i det studieadministrative system. Foreningen vil foreslå, at beskrivelsen af kontrol 20 udvides med henblik på at specificere, at Datatilsynets skabelon til databehandleraftaler skal anvendes, hvis leverandøren af det studieadministrative system behandler personoplysninger på institutionens vegne. Det vil sikre, at artikel 28 stk. 3 litra a) – h) i Databeskyttelsesforordningen, som omhandler forordningens krav til en databehandler, overholdes.

Med venlig hilsen

Maja Bødtcher-Hansen
Formand

Steen Larsen

Fra: Danske HF & VUC <VUC@vuc.dk>
Sendt: 28. oktober 2024 14:14
Til: Steen Larsen
Emne: Høring efterår 2024 – Systemrevisionsbekendtgørelsen [Danske HF & VUC]

[EKSTERN E-MAIL] Denne e-mail er sendt fra en ekstern afsender.
Vær opmærksom på, at den kan indeholde links og vedhæftede dokumenter, som ikke er sikre, medmindre du stoler på afsenderen.

Kære Steen

Tak for muligheden for at afgive høringssvar.

Vi har en enkelt kommentar/et spørgsmål til høringen.

I bilag 1 – punkt 2 *Adgangsstyring og styring af adgang til personoplysninger*

Nr. 4 c. funktionalitet og kontroller til at tjekke anvendte passwords mod negativlister, herunder månedlige kontroller af, om anvendte passwords optræder på velkendte oversigter over lækkede passwords, samt kontroller til forebyggelse af en brugers genbrug af tidligere anvendte passwords

Spørgsmålet er:
Hvilke velkendte oversigter over lækkede passwords, er det ministeriet henviser til? (Der findes mange).

Vh Kirsten

Med venlig hilsen

Kirsten Preisler
Sekretariatschef
Ny Vestergade 17, 3. sal
1471 København K

Mobil: 53 54 07 79
E-mail: kpr@vuc.dk

Fra: Steen Larsen <Steen.Larsen@stil.dk>
Sendt: 1. oktober 2024 14:34
Til: Steen Larsen <Steen.Larsen@stil.dk>
Emne: Høring over udkast til systemrevisionsbekendtgørelse

Høring over udkast til systemrevisionsbekendtgørelse

Børne- og Undervisningsministeriet, Styrelsen for It og Læring, sender hermed vedhæftede udkast til bekendtgørelse i høring.

Bekendtgørelsen vedrører krav til studieadministrative it-systemer for almene voksenuddannelser, erhvervsuddannelser, arbejdsmarkedsuddannelser, de gymnasiale uddannelser, forberedende grunduddannelse m.fl.

Der henvises til vedhæftede høringsbrev.

Høringsfristen er **tirsdag den 29. oktober 2024 kl. 15.00.**

Med venlig hilsen
Steen Larsen
Chefkonsulent

STYRELSEN FOR
IT OG LÆRING

Børne- og Undervisningsministeriet
Kontor for Centrale Uddannelsesregistre
Lyseng Allé 1
8270 Højbjerg
Telefon: +45 89 37 66 66

Direkte telefon: +45 25 23 42 49
Mail: steen.larsen@stil.dk

DATATILSYNET

Styrelsen for It og Læring
Teglholmsgade 1
2450 København SV
Att. Steen Larsen

Sendt med Digital Post til steen.larsen@stil.dk

16. oktober 2024

J.nr. 2024-12-0457
Dok.nr. 651365
Sagsbehandler
Marie Louise Buch-Lassen

Datatilsynet
Carl Jacobsens Vej 35
2500 Valby
T 3319 3200
dt@datatilsynet.dk
datatilsynet.dk

CVR 11883729

Svar på høring over udkast til bekendtgørelse om krav til studieadministrative it-systemer

Datatilsynet har den 1. oktober 2024 modtaget en høring fra Styrelsen for It og Læring over udkast til bekendtgørelse om krav til studieadministrative it-systemer for almene voksenuddannelser, erhvervsuddannelser, arbejdsmarkedsuddannelser, de gymnasiale uddannelser forberedende grunduddannelse m.fl.

Udkastet giver Datatilsynet anledning til følgende bemærkninger:

Vedr. Bilag 1, punkt 2.2. "Adgangsstyring og styring af adgang til personoplysninger"
Datatilsynet henleder i relation til den foreslåede kontrol nr. 4 indledningsvis opmærksomheden på de tekniske minimumskrav for statslige myndigheder[1], på passwordvejledningen[2] fra Center for Cybersikkerhed (CFCS) og på The National Institute of Standards and Technology[3], som Datatilsynet formoder, at STIL allerede har indgående kendskab til.

Datatilsynet formoder også, at der er udarbejdet en bagvedliggende og intern passwordpolitik eller lignende, som - ud over det anførte i bekendtgørelsens bilag - mere konkret beskriver diverse krav til anvendte passwords.

Datatilsynet skal på den baggrund bemærke, at de følgende bemærkninger til udkastet til kontrol nr. 4 ikke kan anses for samtidig at være Datatilsynets godkendelse af eventuelle bagvedliggende og interne politikker, procedurer eller retningslinjer for passwords mv. Datatilsynet har alene forholdt sig til de markerede ændringer i den fremsendte høring med bilag.

Kontrol nr. 4a:
Det fremgår f.eks. af det nyeste udkast til password-guidelines fra NIST, at NIST anbefaler, at mantillader,atASCII-ogUnicode-tegnbliverinkluderetipasswords.Sehttps://pages.nist.gov/800-63-4/sp800-63b.html#passwordver Det kan derfor overvejes, om dette bør tilføjes (evt. blot i en bagvedliggende passwordpolitik og ikke nødvendigvis i bekendtgørelsens bilag), da det giver mulighed for at øge passwordkvaliteten (kompleksitet).

1 https://www.sikkerdigital.dk/Media/638638815823835221/De%20tekniske%20minimumskrav%20oktober%202024.pdf
2 https://www.cfcs.dk/globalassets/cfcs/dokumenter/vejledninger/-passwordsikkerhed-oktober-2023-.pdf
3 https://www.nist.gov/cyberframework

Kontrol nr. 4b og kontrol nr. 4c:
Af det fremsendte udkast fremgår det, at den foreslåede formulering er: "*b. funktionalitet til tvungen udskiftning af password*". Af de tekniske minimumskrav for statslige myndigheder 2024, fremgår følgende på side 12, punkt 2: "*brugerkonti, hvor der anvendes lækkede passwords, tvinges til at skifte password ved næste log-on [..]*". Datatilsynet skal på den baggrund anbefale, at der foretages justeringer i sætningen, og at der tilføjes "*ved næste log-on*".

Af passwordvejledningen fra CFCS fremgår det på side 18 og 19, at CFCS anbefaler, (i) at der benyttes kontospærring eller throttling (forsinkelse på nye loginforsøg), (ii) at organisationen har en fast procedure med krav til genåbning af låste konti, (iii) og at loginforsøg logges og monitoreres. Kontospærring kan være en metode til at hindre, at hackere ved hjælp af et onlineangreb formår at bryde passwords og få adgang til interne it-systemer. Det kan derfor overvejes, om dette bør indgå i beskrivelsen af de konkrete kontroller i nr. 4.

Datatilsynet har ikke yderligere bemærkninger til det fremsendte udkast, men tilsynet forudsætter i øvrigt, at databeskyttelsesforordningens[4] og databeskyttelseslovens[5] bestemmelser, herunder kravene til behandlingssikkerhed, anvendelse af databehandlere, databeskyttelse gennem design og standardindstillinger, konsekvensanalyse og de registreredes rettigheder, vil blive iagttaget i forbindelse med de behandlinger af personoplysninger, der vil ske som følge af bekendtgørelsens bestemmelser.

Afsluttende bemærkninger
Såfremt ovenstående giver anledning til spørgsmål, er STIL velkommen til at rette henvendelse til specialkonsulent Marie Lassen på telefon 29 49 33 03 eller til it-sikkerhedskonsulent Morten Rasmussen på telefon 29 49 32 60.

Med venlig hilsen

Marie Lassen

4 https://eur-lex.europa.eu/legal-content/DA/TXT/PDF/?uri=CELEX:32016R0679&from=DA
5 https://www.retsinformation.dk/eli/lta/2024/289

Steen Larsen

Fra: Henrik Faaborg (HEFA - IT-Chef - EFIF) <hefa@efif.dk>
Sendt: 29. oktober 2024 14:33
Til: Steen Larsen
Cc: Martin Hovbakke Sørensen; Pernille.Frimann.Heiring; Bettina Lundgaard (VORLU - Fuldmægtig - VB - VOR); Rune Gråbæk (RUNE.ZBC - IT- og digitaliseringschef - NATR - ZBC); Ebbe Udengaard (EBUD - Ressourcedirektør - NV - ZBC); Filip Lange (FILA - Ressourcedirektør - U/NORD)
Emne: Høring over udkast til systemrevisionsbekendtgørelse
Vedhæftede filer: Høring efterår 2024.pdf

Kære STIL

Høring efterår 2024 – Systemrevisionsbekendtgørelsen

Børne- og Undervisningsministeriet, Styrelsen for It og Læring, har den 1. oktober 2024 sendt udkast til bekendtgørelse om krav til studieadministrative it-systemer for almene voksenuddannelser, erhvervsuddannelser, arbejdsmarkedsuddannelser, de gymnasiale uddannelser, forberedende grunduddannelse m.fl i høring.

Undertegnende repræsentanter har følgende kommentarer og ønsker til supplerende ændringer. Indledningsvis er det vores vurdering, at det fremsatte udkast til systemrevisionsbekendtgørelse, indeholder mange gode og nye forbedringer. Vi har 2 ønsker og forslag, som er vedlagt i bilag.

Ønsker I at vi skal uddybe vores ønsker og forslag stiller vi os gerne til rådighed.

Venlig hilsen

Learnmark Gymnasium HHX & HTX, Køge Handelsskole, EUC NORD, Uddannelsescenter Holstebro, Holstebro Gymnasium og HF, Campus Bornholm, Vordingborg Gymnasium & HF, Næstved Gymnasium og HF, ZBC, Kolding Gymnasium, Aabenraa Statsskole, Herning Gymnasium, Frederikshavn Gymnasium, Frederikshavn Handelsskole, Frederikssund Gymnasium, Nakskov Gymnasium & HF, Maribo Gymnasium, DPO i Gymnasiefælleskabet og U/NORD

Høring efterår 2024 – Systemrevisionsbekendtgørelsen – "Learnmark Gymnasium HHX & HTX, Køge Handelsskole, EUC NORD, Uddannelsescenter Holstebro, Holstebro Gymnasium og HF, Campus Bornholm, Vordingborg Gymnasium & HF, Næstved Gymnasium og HF, ZBC, Kolding Gymnasium, Aabenraa Statsskole, Herning Gymnasium, Frederikshavn Gymnasium, Frederikshavn Handelsskole, Frederikssund Gymnasium, Nakskov Gymnasium & HF, Maribo Gymnasium, DPO i Gymnasiefælleskabet og U/NORD"

Vi har 2 ønsker og forslag

1)

At der i kontrol nr. 4 i a) foreslås en tilføjelse (markeret med gult) så der står "At brugere til SA-systemet har flerfaktor-autentifikation eller funktionalitet og kontroller til at sikre passwords af tilstrækkelig kvalitet, herunder at anvendte passwords har en længde på 15 tegn eller flere for medarbejdere samt brugere med tilgang til personoplysninger om elever/kursister, lærere og øvrige bruger"

NB: Rettesnor kunne med fordel være at lægge sig op ad statens minimumskrav De tekniske minimumskrav oktober 2024.pdf

2)

Ændringsforslag til udkastet:

I forhold til det fremsatte udkast til systemrevisionsbekendtgørelse foreslås følgende supplerende tilføjelser

I afsnit 2.7 "Behandling af personoplysninger"

kontrol nr. 20 foreslås en tilføjelse (markeret med gult)

Nr. 20 Kontrol:

Systemleverandøren har etableret procedurer til sikring og dokumentation af, at systemets behandling af personoplysninger er i overensstemmelse med gældende databeskyttelsesregler (databeskyttelsesforordningen, databeskyttelsesloven m.v.), herunder for udformning og indgåelse af databehandleraftaler, som overholder kravene i databeskyttelsesforordningens artikel 28, stk. 3, og der som minimum er udformet på baggrund af Datatilsynets til hver en tid gældende skabelon til databehandleraftale, hvis leverandøren af det studieadministrative system behandler personoplysninger i systemet på institutionernes vegne.

De indeholder således detaljeret instruks, beskrivelse af tekniske og organisatoriske sikkerhedsforanstaltninger og dokumentation af et sikkerhedsniveau, der afspejler, hvilke personoplysninger leverandøren behandler i systemet.

En systemgodkendelse fra STIL betyder ikke, at STIL overtager institutionernes tilsynsforpligtelse over for leverandøren i forhold til kontrol af, hvorledes leverandøren efterlever de databeskyttelsesretslige regler. Institutionernes tilsynspligt over for systemleverandøren suspenderes således ikke ved systemgodkendelsen.

Steen Larsen

Fra: Rune Møller Andersen <runan@eg.dk>
Sendt: 15. oktober 2024 11:03
Til: Steen Larsen
Emne: Høring efterår 2024 – Systemrevisionsbekendtgørelsen EG / LUDUS

[EKSTERN E-MAIL] Denne e-mail er sendt fra en ekstern afsender.
Vær opmærksom på, at den kan indeholde links og vedhæftede dokumenter, som ikke er sikre, medmindre du stoler på afsenderen.

Hej Steen
Tak for høringsmaterialet. EG LUDUS har læst materialet igennem og har enkelt kommentar, som vil være meget problematisk for EG LUDUS, afhængig af hvordan den fortolkes.

I kontrol 4 c, skrives der: *funktionalitet og kontroller til at tjekke anvendte passwords mod negativlister, herunder månedlige kontroller af, om anvendte passwords optræder på velkendte oversigter over lækkede passwords, samt kontroller til forebyggelse af en brugers genbrug af tidligere anvendte passwords*

Hvis hensigten med kontrollen er at vi bogstavligt skal kontrollere passwords, vil dette være en udfordring, da EG LUDUS gemmer brugernes password i løsningen som hashede værdier. Det betyder at vi ikke er i stand til at genskabe deres klartekst værdi, og derfor ikke kan lave en månedlig kontrol.

Endvidere anbefaler CFCS at man ikke kontrollere passwords som er i anvendelse.
https://www.cfcs.dk/globalassets/cfcs/dokumenter/vejledninger/-passwordsikkerhed-oktober-2023-.pdf
nederst side 7

Men hvis hensigten med kontrollen, er at kontrollere om selv brugerkontoen med brugernavn og password, står registeret som lækket, så vurdere vi godt at der kan etableres en kontrol i EG LUDUS.

Generelt synes vi i EG har man bør læne sig op af de retningslinjer om center for cybersikkerhed anbefaler, for password sikkerhed.

Venlig hilsen / best regards

Rune Møller Andersen
Senior Operations Manager
EG Digital Welfare

EG Digital Welfare ApS - Østerbro 5 B, st. tv - 5000 Odense
T: +45 6617 7313 - D: +45 7260 2692
M: +45 5190 6936
E-mail: runan@eg.dk - web: www.eg.dk
Read our Privacy Policy

Steen Larsen

Fra: Dorte Holm Phillip <dorte.holm@ist.com>
Sendt: 21. oktober 2024 10:44
Til: Steen Larsen
Emne: Ny systembekendtgørelse

[EKSTERN E-MAIL] Denne e-mail er sendt fra en ekstern afsender.
Vær opmærksom på, at den kan indeholde links og vedhæftede dokumenter, som ikke er sikre, medmindre du stoler på afsenderen.

Hej Steen

Vi er jo ikke direkte blevet bedt om kommentarer til den systembekendtgørelse, som er sendt i høring. Men du får lige vores kommentarer alligevel, da du ellers får dem senere som spørgsmål, når jeg står med revisoren 😊

Afsnit 2.2 Krav 4
c. Password skal da tjekkes når det tastes første gang og ikke kun senere? Vi vil gerne have specificeret listerne, hvad er velkendt?
e. Vi forstår ikke hvad der menes? Må koden komme i en APP?
a. og **d.** er modstridende. Vi vil gerne have præciseret i hvilke tilfælde password reglerne må bruges og er relevante, og hvornår MFA er påkrævet. Er passwordkravene også gældende ved en MFA løsning?
Må vi bruge MitID som MFA løsning?

Afsnit 4.32 krav 103 GYM-henvisningstilskud skal væk, den findes ikke længere.

Nyt forslag: Bør der være krav ud over dem som AUB og US2000 allerede har, til struktureret og dokumenteret data overdragelse og overtagelse af data ved leverandørskift.
Hvilke data skal overdrages?

Med venlig hilsen

Dorte Holm Phillip
Head of Development and Operation

M +45 7222 6110
T +45 7222 6110

IST Danmark ApS
Lindevej 5A · 5750 Ringe · Danmark
www.ist.com

Please note that this message may contain confidential information. If you have received this message by mistake, please inform the sender of the mistake by sending a reply, then delete the message from your system without making, distributing or retaining any copies of it. If you want to know how we at IST process your personal data please read our Privacy Policy at https://www.ist.com/en/policy