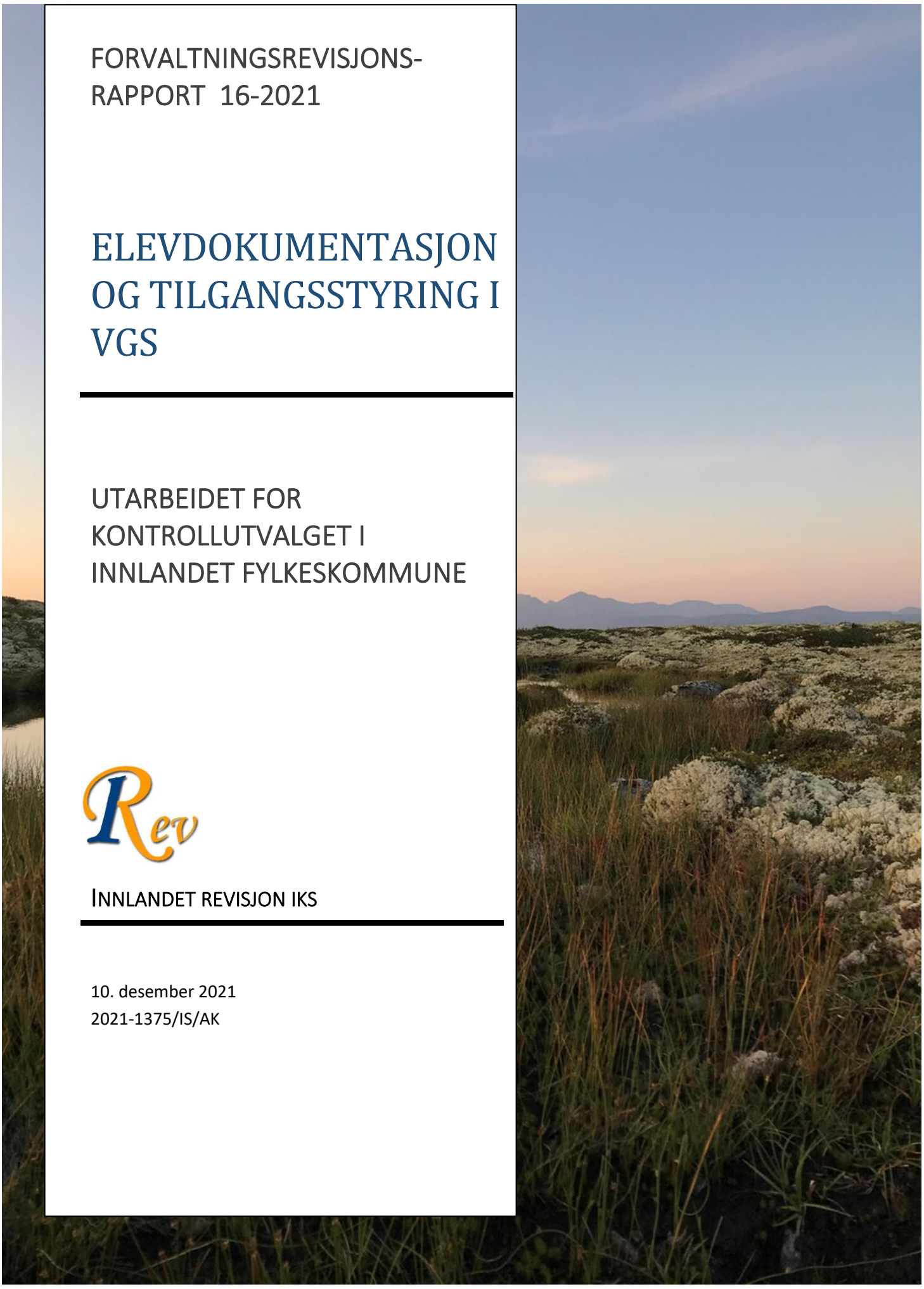
FORVALTNINGSREVISJONS-
RAPPORT 16-2021

ELEVDOKUMENTASJON OG TILGANGSSTYRING I VGS

UTARBEIDET FOR
KONTROLLUTVALGET I
INNLANDET FYLKESKOMMUNE



INNLANDET REVISJON IKS

10. desember 2021
2021-1375/IS/AK

FORORD

Denne rapporten er et resultat av forvaltningsrevisjonsprosjektet *Elevdokumentasjon og tilgangsstyring* som er gjennomført på oppdrag av kontrollutvalget i Innlandet fylkeskommune.

Forvaltningsrevisjon er en lovpålagt oppgave som innebærer å gjennomføre systematiske vurderinger av økonomi, produktivitet, regeletterlevelse, måloppnåelse og virkninger ut fra kommunestyrets eller fylkestingets vedtak (Kommunelovens § 23-3.).

Prosjektarbeidet er utført i perioden desember 2020 til november 2021 av forvaltningsrevisor Anette Karenstuen. Ingvild Selfors er oppdragsansvarlig revisor og Reidun Grefsrud har kvalitetssikret rapporten.

Utkast til rapport er sendt fylkeskommunedirektøren til uttalelse. Svaret fra fylkeskommunedirektøren er vedlagt rapporten. På bakgrunn av fylkeskommunedirektørens uttalelse er det gjort små rettinger i rapporten.[1]

Vi takker for godt samarbeid med ansatte i fylkeskommunen og videregående skole som vi har hatt kontakt med i prosjektarbeidet.

Lillehammer 10. desember 2021

Ingvild Selfors

Ingvild Selfors
Oppdragsansvarlig revisor

Anette Karenstuen

Anette Karenstuen
Prosjektansvarlig revisor

[1] Dette gjelder elevtall på Storsteigen VGS og nummerering av revisjonskriterier og anbefalinger.

INNHOLD

SAMMENDRAG

Formålet med revisjonen er å sette fokus på tilgangsstyring i sentrale IKT-systemer i videregående opplæring i Innlandet fylkeskommune.

Revisjonskriteriene er i hovedsak hentet fra personopplysningsloven med EUs personvernforordning, kommuneloven og fylkeskommunens egne styringsdokumenter som omhandler tilgangsstyring og ivaretakelse av personvern. For å utlede konkrete revisjonskriterier har vi tatt utgangspunkt i anerkjente standarder og veiledninger på området, herunder Datatilsynets veiledning om plikter etter personvernregleverket, Nasjonal sikkerhetsmyndighets grunnprinsipper for IKT-sikkerhet og ISO/IEC 27001– Ledelsessystem for IKT-sikkerhet.

Revisjonen har valgt å se nærmere på IKT-systemene Visma InSchool, ViGO, Conexus Engage og Oppfølgingsloggen. Faktaopplysninger i rapporten er i hovedsak innhentet ved intervjuer og gjennomgang av tilganger i de utvalgte IKT-systemene. Revisjonen har også innhentet relevante dokumenter og rutiner fra fylkeskommunen.

Problemstillinger med tilhørende hovedkonklusjoner og et utdrag av konklusjonene er gjengitt nedenfor:

Problemstilling 1

Hvilke IKT-systemer behandler personopplysninger om elever i videregående opplæring og hvilke personopplysninger behandles i disse systemene?

Revisjonen har kartlagt hvilke IKT-systemer som behandler personopplysninger om elever i videregående opplæring og hvilke personopplysninger som behandles i disse systemene.

Det er omtrent 150 systemer eller applikasjoner som behandler personopplysninger om elever i de videregående skolene. Dette inkluderer digitale læremidler, pedagogiske læremidler og andre programmer/nettbaserte tjenester som krever at bruker logger på, men hvor det er svært begrenset med personopplysninger som lagres.

IKT-systemer der elevdokumentasjon registreres og behandles er VIGO, Visma InSchool, Engage, Oppfølgingsloggen, Elements, Microsoft Office 365 og LAO. Disse IKT-systemene lagrer og behandler store menger av personopplysninger om elever. Det er i hovedsak Elements, LAO, og Oppfølgingsloggen som behandler sensitive personopplysninger om elever.

Problemstilling 2

I hvilken grad har fylkeskommunen etablert grunnleggende retningslinjer og rutiner for tilgangsstyring?

Revisjonens hovedkonklusjon er at fylkeskommunen i mindre grad har etablert grunnleggende retningslinjer og rutiner for tilgangsstyring som bør være på plass for at tilgangsstyringen skal fungere best mulig.

Fylkeskommunen har på nåværende tidspunkt ingen overordnet retningslinje for tilgangsstyring, selv om de har på plass enkelte deler av hva en overordnet rutine bør inneholde. Det mangler tydelig ansvarsfordeling innen tilgangskontrollen og det foreligger ingen rutine for jevnlig gjennomgang av brukerrettigheter.

Feide og ID-porten benyttes for innlogging i IKT-systemer som behandler elevdokumentasjon. Fylkeskommunen har en formell passordpolicy som er innbakt i systemene og det er ikke mulig å opprette passord i strid med kravene. Selv om fylkeskommunen har implementert passordregler så finnes det ikke noe skriftlig på dette området, noe som vurderes å være en svakhet. Grunnleggende retningslinjer og rutiner for tilgangsstyring burde også sagt noe om hvilke opplysninger og systemer som skulle vært beskyttet av to-faktorautentisering, dette mangler.

Fylkeskommunen har ingen aktiv sikkerhetsovervåkning i systemene for å oppdage eventuelle innbrudd i systemene.

Problemstilling 3

I hvilken grad er det etablert tilfredsstillende tiltak for tilgangsstyring i utvalgte IKT-systemer som behandler personopplysninger om elever, og i hvilken grad er disse etterlevd?

I problemstilling 3 har revisjonen undersøkt den faktiske tilgangsstyringen i IKT-systemene Visma InSchool, Conexus Engage og Oppfølgingsloggen, og VIGO, basert på etablert praksis i seks videregående skoler.

Vår hovedkonklusjon er at fylkeskommunen i mindre grad har etablert tilfredsstillende tiltak for tilgangsstyring i utvalgte IKT-systemer som behandler personopplysninger om elever. Det er i liten grad dokumenterte og operasjonaliserte rutiner for tilgangsstyring, noe som kan synes å påvirke praksis for opprettelse, vedlikehold og avslutning av brukerkontoer ute på skolene. Av IKT-systemene som ble undersøkt er det kun Visma InSchool som har dokumentert hvordan arbeidet med tilgangsstyring skal gjennomføres.

Det er ikke satt i verk to-faktor autentisering i IKT-systemer som bruker Feide for innlogging, herunder Visma InSchool og Engage. Dette er systemer som behandler store mengder personopplysninger på vegne av elever i videregående skole. Videre er administratortilgang knyttet til vanlige brukerkontoer i alle systemene som er undersøkt, noe som gir større risiko dersom uvedkommende skulle få tilgang til brukerkontoen. Ved at innloggingen til IKT-systemene Engage og Visma in School er eksponert direkte på internett synes det å være en stor risiko ved at to-faktorautentisering ikke er iverksatt.

Ansvarlige for tilgangsstyring i IKT-systemene ute på skolene var opptatt av at tilganger skal være i samsvar med tjenstlig behov, noe revisjonen vurderer som positivt. Samtidig så revisjonen i gjennomgangen av tilganger at det forelå administratortilganger i større utstrekning enn det var tjenstlig behov for i IKT- systemene Visma InSchool, Engage og VIGO, noe som kan tyde på at det ikke er tilstrekkelig kontroll på administratorkontoer.

På grunnlag av vurderinger og konklusjoner har revisjonen følgende anbefalinger:

1. Fylkeskommunen bør utarbeide og implementere overordnet retningslinje for tilgangskontroll basert på en overordnet informasjonsklassifisering. Retningslinjen bør inneholde følgende punkter:
    a. Tilgang tildeles i samsvar med tjenstlig behov, herunder vurdering av hvilken tilgang som er nødvendig.
    b. Rutiner for tildeling, endring, sletting og kontroll av tilganger.
    c. Rutiner for autentisering basert på graden av sensitivitet i personopplysningene og hvilken enhet pålogging skjer fra.
    d. Tildeling av rettighet til tilgang (autorisasjon) skal registreres i et register.
    e. Ansvarsfordeling innen tilgangskontrollen
2. For å sikre personopplysninger om elever i IKT-systemer som behandler sensitive personopplysninger og/eller store mengder personopplysninger, bør fylkeskommunen iverksette to-faktor autentisering i Feide.
3. Fylkeskommunen bør iverksette sikkerhetsovervåking for å oppdage sikkerhetshendelser knyttet til tilgangskontrollen.
4. Administratorprivilegier bør ha separate brukerkontoer dersom det er teknisk gjennomførbart. Som minimum bør administratorkontoer være beskyttet av to-faktor autentisering.
5. Fylkeskommunen bør sørge for jevnlig kontroll av tilganger i IKT-systemer som behandler elevdokumentasjon, spesielt tilganger med utvidete rettigheter (administratortilganger).
6. Fylkeskommunen bør innrette tilgangsstyringen i IKT-systemene i henhold til risikovurdering av informasjonsverdiene i systemet.

1 INNLEDNING

1.1 KONTROLLUTVALGETS BESTILLING

Kontrollutvalget vedtok følgende i sak 34/2020, den 03.09.2020:

1. *Kontrollutvalget bestiller to forvaltningsrevisjoner basert på den fremlagte foranalysen «IKT-anskaffelser og sikkerhet» med følgende tema:*
    - *Ivaretagelse av informasjonssikkerheten i sentrale IKT-systemer hvor formålet skal være å bidra til å sette fokus på informasjonssikkerheten i sentrale IKT-systemer i fylkeskommunen.*
    - *Elevdokumentasjon og tilgangskontroller hvor formålet skal være å sette fokus på tilgangskontroller i sentrale IKT-systemer i de videregående skolene.*
2. *Kontrollutvalget ønsker at prosjektplaner for begge temaene legges fram på neste møte den 15.10.2020.*

Denne rapporten gjelder det andre kulepunktet i bestillingen: *Elevdokumentasjon og tilgangskontroller, hvor formålet skal være å sette fokus på tilgangskontroller i sentrale IKT-systemer i de videregående skolene.*

Innlandet Revisjon IKS utarbeidet en prosjektplan som ble lagt frem for kontrollutvalget den 15.10.2020.

1.2 FORMÅL OG PROBLEMSTILLINGER

Formålet med revisjonen er å sette fokus på tilgangsstyring i utvalgte IKT-systemer i videregående opplæring i Innlandet fylkeskommune. Det er formulert følgende problemstillinger for prosjektet:

Problemstilling 1:
Hvilke IKT-systemer behandler personopplysninger om elever i videregående opplæring, og hvilke personopplysninger behandles i de ulike IKT- systemene?

Problemstilling 2:
I hvilken grad er det etablert grunnleggende retningslinjer og rutiner for tilgangsstyring i IKT-systemer som behandler elevdokumentasjon?

Problemstilling 3:
I hvilken grad er det etablert rutiner og praksis for kontroll av tilgangsstyringen i utvalgte IKT-systemer som behandler personopplysninger om elever i videregående opplæring?

Det er gjort noen justeringer i ordlyden i forhold til den opprinnelige formuleringen i prosjektplanen. Justeringen innebærer ingen praktiske endringer for revisjonsarbeidet.

I problemstilling 1 kartlegger vi hvilke IKT-systemer som brukes til å behandle personopplysninger om elever og hvilke typer opplysninger som blir behandlet i de ulike systemene. I tillegg kartlegger vi hvor systemene benyttes. Med dette mener vi å finne ut hvilke systemer som bare benyttes sentralt i fylket, hvilke systemer som bare

benyttes i skolene, og om det kan være ulike systemer i bruk fra skole til skole. Resultatene fra kartleggingen danner grunnlag for å velge ut et antall skoler og aktuelle IKT-systemer for videre gjennomgang i problemstilling 3.

I problemstilling 2 undersøker vi om fylkeskommunen har overordnede retningslinjer, rutiner og generell dokumentasjon som bør være på plass for at tilgangsstyringen skal fungere best mulig.

Den faktiske tilgangsstyringen i utvalgte IKT-systemer som behandler personopplysninger om elever i de videregående skolene undersøkes i problemstilling 3. Her vurderer vi om fylkeskommunen har etablert tilfredsstillende tiltak for tilgangsstyring, samt i hvilken grad dette er kjent og etterlevd i praksis. Utvalget av IKT-systemer baserer seg på informasjonen fra kartleggingen i problemstilling 1, og omfatter systemer som behandler sensitive opplysninger om elever og/eller personopplysninger om elever i et stort omfang.

1.2.1 AVGRENSNING

Det er kun elektronisk behandling av personopplysninger som blir undersøkt. Hvordan tilgangsstyring er ivaretatt for personopplysninger som er lagret i papirform undersøkes ikke. Videre fokuserer prosjektet kun på personopplysninger som er lagret om elever og ikke om ansatte i fylkeskommunen.

1.3 ELEVDOKUMENTASJON OG TILGANGSSTYRING

I det følgende redegjør vi for begrepene elevdokumentasjon og tilgangsstyring. Herunder hvilke typer opplysninger som lagres om elever i videregående skole, samt hva tilgangsstyring er og hvorfor det er viktig i møte med IKT-systemer som behandler elevdokumentasjon

1.3.1 ELEVDOKUMENTASJON

Fylkeskommunen og de videregående skolene oppbevarer og behandler store mengder personopplysninger på vegne av elever. De har blant annet opplysninger om hvilke elever som har gått på hvilken skole, fravær, undervisningsvurderinger, sluttvurderinger, karakterer og elevbesvarelser. Det er ikke bare de opplysningene som tradisjonelt har vært lagret om elever som er å anse som personopplysninger. I dag er det mye mer som lagres i skolen som kan knyttes til elever; bilder, kommunikasjon mellom elever, kommunikasjon mellom lærer og elev, kommunikasjon mellom skole og hjem, informasjon om helseforhold som allergier, logg fra elevenes bruk av skolens nettverk, logg fra elevenes bruk av pedagogiske verktøy og lignende.

I tillegg lagres det særlige kategorier personopplysninger som enkeltvedtak, opplysninger om sykdom og helseforhold, vurderinger, referater fra samarbeid med BUP, PPT og helsevesen, etc. Samlet utgjør dette et sett med opplysninger som gir et omfattende og detaljert bilde av elevens utvikling og dens faglige og sosiale atferd gjennom et helt utdannelsesløp.[2] Det er derfor viktig at skolene har kontroll på disse opplysningene og med hvem som har tilgang til hvilke opplysninger.

[2] Datatilsynet, "Personvern i skole og barnehage", Samlerapport, juni 2014

Personvernforordningens fortalepunkt[3] 38 fastslår at barns personopplysninger på generelt grunnlag fortjener særlig vern, ettersom barn kan være mindre bevisst på aktuelle risikoer, konsekvenser og garantier, samt på de rettigheter de har når det gjelder personopplysninger.[4]

1.3.2 TILGANGSSTYRING

Informasjonssikkerhet knyttet til IKT-systemer omfatter fysiske, systemtekniske og organisatoriske tiltak for å sikre at informasjonen er hemmelig for uautoriserte brukere (konfidensialitet), at den er korrekt og pålitelig (integritet), og at den er tilgjengelig når man trenger den (tilgjengelighet). *Tilgangsstyring* er et sikkerhetstiltak som skal bidra til å oppfylle målene om konfidensialitet, integritet og tilgjengelighet for virksomhetens informasjon.

Tilgangsstyring innebærer å bare tildele godkjent personell, brukere eller maskiner tilgang til et system, et domene eller et konkret sett med opplysninger. Et regelsett må opprettes for å kunne fastsette hvem som skal få se eller redigere hva. For å sikre at kun rett personell får tilgang i henhold til regelsettet som fastsetter roller og tilgang, må en form for autentisering benyttes. Dersom brukeren kan bevise at han faktisk er den han utgir seg for, og dersom det er vurdert at vedkommende har et faktisk behov for autorisasjon, skal brukeren gis tilgang til opplysningene[5].

Datatilsynet beskriver i sin samlerapport om personvern og barnehage (2014)[6] at de normalt anser innlogging ved brukernavn og passord som tilstrekkelig sikkert, for *foresatte og barns* tilgang til læringsplattformer og kommunikasjonsplattformer. Når det gjelder tilgangen for de *ansatte* vurderte de det derimot slik at det må kreves en sterkere autentisering – og særlig når tilgang er mulig fra eksterne nett eller elevnett. Kravet om strengere sikkerhet ved ansattes innlogging utenfor skolens/barnehagens nettverk er begrunnet med at en ansatt ved innlogging på en læringsplattform, skoleadministrativt system eller kommunikasjonsplattform får tilgang til personopplysninger om svært mange barn. Med sterk autentisering mener de for eksempel bruk av kodebrikke eller sikkerhetskode tilsendt på SMS.

Datatilsynet beskriver videre i sin årsrapport fra 2019 at de gjennom avviksmeldinger som har kommet inn har sett at det er en rekke hendelser som berører personvernet til barn og unge i skolen. De har blant annet sett flere tilfeller knyttet til mangelfull tilgangsstyring til informasjonssystem med opplysninger om elever, herunder i læringsplattformer og i skole-administrative systemer. Også manglende to-faktor autentisering, menneskelig svikt og manglende rutiner går igjen i avviksmeldinger som er meldt Datatilsynet. Datatilsynet har per januar 2020 flere alvorlige avvikssaker som berører barn og unge under behandling. I sin årsrapport for 2020 skriver Datatilsynet at de har videreført arbeidet med å styrke personvernet til barn og unge i offentlig sektor. De beskriver at det er et utfordringsbilde i sakene de har behandlet at det fortsatt er liten kompetanse blant ansatte i stat, kommune og fylkeskommune om barns særskilte beskyttelsesvern etter personvernregelverket.

Manglende tilgangsstyring kan gjøre det vanskelig å kontrollere og forvalte tilgang til kritiske tjenester og data. Dersom personer har tilgang til systemer, tjenester og dokumentasjon de ikke har tjenstlig behov for kan dette

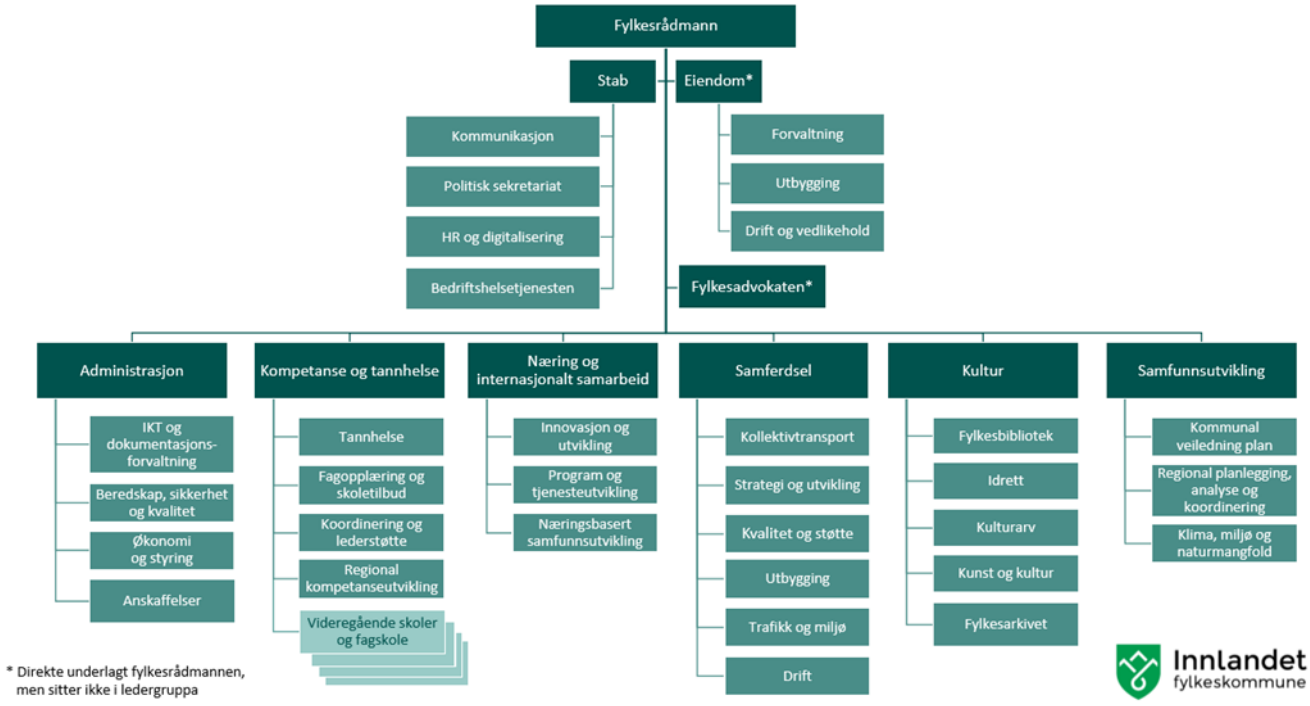
---

[3] Forarbeider til personvernforordningen.
[4] Prop. 56 LS s 96.
[5] https://snl.no/tilgangskontroll_-_informasjonssikkerhet
[6] skoleprosjektet_samlerapport.pdf (datatilsynet.no)

føre til brudd på målene for IKT-sikkerhet om integritet og konfidensialitet. Riktig tilgangsstyring er i tillegg viktig for å redusere skadene ved en eventuell uautorisert tilgang. Dersom en angriper får tilgang til et av fylkeskommunens IKT-systemer vil vedkommende ofte forsøke å øke tilgangen. Dette gjøres som regel ved å ta over ulike kontoer for å eskalere rettigheter. Dersom alle brukere har tilgang til all informasjon vil kompromittering av én bruker kompromittere hele IKT-systemet, og sensitiv elevdokumentasjon vil kunne komme på avveie.[7]

Østre-Toten kommune ble i januar 2021 utsatt for et stort dataangrep. Kommunedirektør i Østre-Toten kommune beskrev i Oppland Arbeiderblad at undersøkelsene etter angrepet avdekket at hackerne benyttet en bruker-ID med administratortilgang til å komme seg innenfor og rundt i kommunens systemer. Undersøkelsene avdekket også at kommunen ikke hadde et godt nok system for administrering og tilgangsstyring på administrator-ID-er. [8]

1.4 ORGANISERING



Hedmark og Oppland fylkeskommuner ble slått sammen til Innlandet fylkeskommune 1. januar 2020. Fylkeskommunedirektøren er fylkeskommunens øverste administrative leder. I tillegg til stabs- og eiendomsavdelingene er fylkeskommunen organisert i seks avdelinger: Administrasjonsavdeling, avdeling

[7] Nasjonal sikkerhetsmyndighet, "NSMs Grunnprinsipper for IKT-sikkerhet versjon 2.0", ferdigstilt 15. april 2020

[8] Oppland Arbeiderblad «PYSA-banden hadde administrator-ID til Østre Totens datasystemer» 27.08.2021.

for Kompetanse og tannhelse, avdeling for Næring og internasjonalt samarbeid, avdeling for Samferdsel, avdeling for Kultur og avdeling for Samfunnsutvikling. Avdelingene består av flere seksjoner og underenheter.

Innlandet fylkeskommune har ca. 4000 ansatte. Fylkeskommunen eier og drifter 23 videregående skoler, Fagskolen Innlandet, to folkehøgskoler, karrieresentre, 41 tannklinikker, nesten 7000 km fylkesveger, og har ansvaret for kollektivtrafikken i fylket gjennom Innlandstrafikk. Sentraladministrasjonen er delt på to lokasjoner – Lillehammer og Hamar.

Seksjonssjef for Koordinering og lederstøtte i avdeling for Kompetanse og tannhelse har personalansvar for rektorene ved de videregående skolene. Det er store forskjeller på skolestørrelser i fylkeskommunen, fra Storsteigen VGS med 120 elever til Hamar Katedralskole med 1156 elever. Dette påvirker hvordan de organiserer arbeidet med IKT og tilgangsstyring. På små skoler vil en ansatt kunne inneha mange roller i et IKT-system og ha tjenstlig behov for omfattende tilganger, mens på store skoler vil ansvaret fordeles på flere, og den enkelte ansatte inneha færre roller.

Revisjonen tar for seg to nivåer. Fylkeskommunen som skoleeier og skolene. Ifølge dokumentet *«Roller og ansvar for informasjonssikkerhet og personvern»* har fylkeskommunedirektøren det overordnede ansvaret for personvern og informasjonssikkerhet i organisasjonen. Herunder ivareta fylkeskommunens plikter som behandlingsansvarlig etter personopplysningsloven og myndighet til å styre og akseptere all risiko i Innlandet fylkeskommune. Fylkeskommunedirektør har det overordnede ansvaret for at styringssystem for personvern og informasjonssikkerhet realiseres og etterleves.

Når det gjelder ansvar for IKT-systemer knyttet til fylkeskommunens digitale tjenester fordeles ansvaret mellom tjenesteeier (ofte kalt systemeier) og tjenesteansvarlig (ofte kalt systemansvarlig).

Tjenesteeier (systemeier) innehar en lederrolle i virksomheten og har det overordnede ansvaret for informasjonssikkerhet og personvern innenfor den konkrete tjenesten. Tjenesteeier er bestiller/funksjonell premissgiver innen tjenestens funksjonsområde, og setter rammene for tjenesteutviklingen og er ansvarlig for å dokumentere at informasjonssikkerhet og personvern er ivaretatt i tjenesten henhold til standard for risikostyring.

Tjenesteansvarlig (systemansvarlig) ivaretar de daglige oppgavene knyttet til informasjonssikkerhet og personvern gjennom å identifisere, iverksette og kontrollere tjenesten. Tjenesteansvarlig skal rapportere sikkerhetsavvik til tjenesteeier.

For de omtalte IKT-systemene i dette prosjektet er tjenesteeier (systemeier) og tjenesteansvarlig (systemansvarlig) organisatorisk plassert i sentraladministrasjonen i fylkeskommunen. Det er videre lokale skoleadministratorer som er organisatorisk plassert på skolene.

2 METODE

I dette kapittelet beskriver og drøfter vi hvordan vi har gått frem i våre undersøkelser.

Oppstartsmøte for prosjektet ble avholdt 9. desember 2020. Hilde Grundt (personvernkoordinator, avdeling for Kompetanse og tannhelse), Paal Morken Andersen (enhetsleder Skoleutvikling, avdeling for Kompetanse og tannhelse), Wenche Holen (prosjektleder innføring av Visma InSchool, avdeling for Kompetanse og tannhelse), Britt Karin Rotmo (Pedagogisk bruk av IKT og digitale løsninger i skolene, avdeling for Kompetanse og tannhelse) og Anne Kristin Huse (Pedagogisk bruk av IKT og digitale løsninger i skolene, avdeling for Kompetanse og tannhelse) fra Innlandet fylkeskommune, og forvaltningsrevisorene Ingvild Selfors og Anette Karenstuen fra Innlandet Revisjon deltok på møtet. Et referat fra oppstartsmøtet ble sendt fylkeskommunen for verifisering.

De konkrete revisjonskriteriene ble gjennomgått med revidert enhet via Teams 16.03.2021.

Revisjonen har knyttet til seg ekstern ekspertise for å kvalitetssikre revisjonskriterier, metode og vurderinger, jf. prosjektplanen. Det ble opprettet kontakt med selskapet Diri som leverer tjenester knyttet til informasjonssikkerhet, og som springer ut av informasjonssikkerhetsmiljøet ved NTNU i Gjøvik. Konsulenten som har vært benyttet i forvaltningsrevisjonen er Gaute Wangen.

Faktaopplysninger i rapporten er i hovedsak innhentet ved intervjuer og gjennomgang av tilganger i de utvalgte IKT-systemene. På grunn av koronapandemien har de fleste samtalene med personer i fylkeskommunen foregått via videosamtaler. Revisjonen har også innhentet relevante dokumenter og rutiner fra fylkeskommunen.

Problemstilling 1

For å besvare problemstilling 1 fikk vi oversikt over de aktuelle IKT-systemene fra personvernkoordinator i Innlandet fylkeskommune. Videre hadde vi et forberedende møte med Britt Karin Rotmo og Anne Kristin Huse, der vi fikk et generelt overblikk over systemene og kontaktopplysninger til systemeiere/ansvarlige for de aktuelle systemene i fylkeskommunen. Vi sendte skriftlige spørsmål til de navngitte ansatte per e-post.

Problemstilling 2

For å besvare problemstilling 2 har revisjonen hatt intervju med informasjonssikkerhet- og personvernrådgiver i avdeling for Kvalitet, sikkerhet og beredskap og intervju med rådgiver i avdeling for IKT og dokumentasjonsforvaltning.

Vi har videre hatt dialog med personvernkoordinator i IFK, enhetsleder Drift og leveranse i avdeling for IKT og dokumentasjonsforvaltning, og enhetsleder for Digitale tjenester i avdeling for Kompetanse og tannhelse. Vi har også innhentet informasjon fra HR avdelingen i fylkeskommunen om hvordan ansattes brukerkontoer blir opprettet, endret og slettet. Revisjonen har i tillegg brukt opplysninger gitt i forbindelse med prosjektet «Informasjonssikkerhet i IKT-systemer» til å besvare problemstillingen.

Følgende dokumenter har blitt gjennomgått i forbindelse med problemsstilling 2:

- Databehandleravtale mellom VIGO IKS, IST International Software Technology AS og Oppland fylkeskommune, 2019
- Databehandleravtale mellom VIGO IKS, IST International Software Technology AS og Hedmark fylkeskommune, 2019
- Databehandleravtale mellom Conexus Engage og Innlandet fylkeskommune, datert 26.04.2021
- Databehandleravtale mellom Visma Enterprise AS og Innlandet fylkeskommune, 2020
- To endringsvedlegg til databehandleravtale mellom Visma Enterprise AS og Innlandet fylkeskommune av 06.01.2021 og 22.02.2021.

Problemstilling 3

Revisjonen har i forbindelse med problemstilling 3 valgt å undersøke nærmere tilgangsstyringen i IKT-systemene Visma InSchool, Conexus Engage og Oppfølgingsloggen, og VIGO. Vi har valgt å ikke se nærmere på Elements da dette systemet blir undersøkt i revisjonsprosjektet om «Informasjonssikkerhet i IKT-systemer». Læringsplattformene ItsLearning og Fronter er faset ut og er ikke i bruk fra skoleåret 2021/2022. Revisjonen har derfor vurdert det som mindre relevant å gjøre en revisjon av disse systemene. Når det gjelder applikasjonen Teams i Office 365 har revisjonen blitt informert om at det opprettes nye teams med nye tilganger fra skoleåret 2021/2022, vi har derfor vurdert at det er for tidlig med en revisjon av dette systemet. LAO benyttes kun av skoler i tidligere Oppland fylke.

Vi har plukket ut seks skoler for å undersøke tilgangsstyringen i systemene Visma InSchool, Conexus Engage og Oppfølgingsloggen, og VIGO. Vi har valgt tre skoler fra hvert av de tidligere fylkene basert på skolestørrelse. Det vil si at vi har sett nærmere på to små skoler (Jønsberg VGS og Dokka VGS), to mellomstore skoler (Vinstra VGS og Solør VGS) og to store skoler (Gjøvik VGS og Hamar Katedralskole).

For å undersøke problemstilling 3 har revisjonen intervjuet de som har spesielt ansvar eller kjennskap til IKT-systemene Visma InSchool, VIGO og Conexus Engage og Oppfølgingsloggen i sentraladministrasjonen i fylkeskommunen, totalt tre ansatte. Videre har vi hatt intervju med den eller de ved de utvalgte videregående skolene som har ansvar for tilgangsstyringen i systemene (lokal skoleadministrator), dette tilsvarer 18 intervjuer med skolene. Totalt har vi gjennomført 21 intervjuer i arbeidet med problemstilling 3. I forbindelse med intervjuene undersøkte vi et utvalg tilganger i systemene for å se om tilgangene var iht. tjenstlig behov. Fremgangsmåten for undersøkelsene i det enkelte IKT-system fremgår i fakta kapittelet. Intervjuene ble gjennomført våren 2021.

Følgende dokumenter har blitt gjennomgått i arbeidet med problemstilling 3:

- Rutine for tilgangsstyring - Visma InSchool, oversendt 21.04.2021
- Oversikt over alle tilganger som er knyttet til de ulike rollene i Visma InSchool, datert 18. mars 2021
- Konsekvensvurdering for personvern i Engage, 13.10.2020
- Verdivurdering Engage, oppdatert 28.05.2020.
- Tidlig innsats når det gjelder, IKO – en modell for systematisk frafallsforebygging, 2019.
- Intern beskrivelse av hvordan man går frem for å legge til en ny bruker i VIGO Opplæring.

Revisjonen har i tillegg hatt dialog med enhetsleder for Digitale tjenester i forbindelse med problemstilling 3.

Kvalitetssikring – relevans og pålitelighet

Prosjektet er gjennomført i henhold til RSK 001 Standard for forvaltningsrevisjon som er gjeldende som god kommunal revisjonsskikk fastsatt av Norges kommunerevisorforening. Innlandet Revisjon IKS har et internt kvalitetssikringssystem som er i samsvar med RSK 001.

Datas relevans er knyttet til om undersøkelsen representerer den virkelige situasjonen. Vi mener data som er samlet inn i denne undersøkelsen er egnet til å svare på problemstillingene. Det er likevel viktig å være oppmerksom på at de opplysninger som framkommer i rapporten nødvendigvis er et utvalg av fakta. I problemstilling 3 har vi har sett på praksis i 6 av 23 skoler, og undersøkt fire IKT-systemer. Våre resultater gir derfor kun en pekepinn på praksisen i skolene i Innlandet fylkeskommune

Med pålitelighet menes at data skal være mest mulig presise og nøyaktige. Dette er blant annet ivaretatt ved verifisering av intervjureferater, ved at fakta-kapittelet har vært sendt til fylkeskommunen for gjennomgang og ved innhenting av uttalelse fra kommunedirektøren på utkast til rapport.

3 REVISJONSKRITERIER

Revisjonskriterieriene er grunnlaget for revisjonens vurderinger. Revisjonskriterier skal utledes fra autoritative eller anerkjente kilder. Dette kan være lovbestemmelser, forskrifter, kommunale retningslinjer, kommunale vedtak, faglige standarder mv., som sier noe om hvordan virksomheten skal eller bør drives. Revisjonskriteriene skal være relevante, konkrete og i samsvar med kravene som gjelder innenfor den aktuelle tidsperioden.

Vi har benyttet følgende kilder for revisjonskriterier:

- Personopplysningsloven og personvernforordningen (GDPR)
- Kommuneloven kap. 25
- Fylkeskommunens egne styringsdokumenter som omhandler tilgangsstyring og ivaretagelse av personvern
- Datatilsynets veiledning om virksomheters plikter etter personvernregelverket
- Nasjonal sikkerhetsmyndighets grunnprinsipper for IKT-sikkerhet versjon 2.0
- ISO/IEC 27001 - Ledelsessystem for IKT-sikkerhet

Vi utleder ikke revisjonskriterier for problemstilling 1, da denne er utformet for å kartlegge hvilke IKT- systemer som behandler personopplysninger om elever i videregående skoler i Innlandet fylkeskommune.

3.1 UTLEDNING AV REVISJONSKRITERIER

3.1.1 PERSONOPPLYSNINGSLOVEN

Personopplysningsloven med EUs personvernforordning

Personopplysningsloven består av nasjonale regler og EUs personvernforordning (også kalt GDPR – General Data Protection Regulation). EUs personvernforordning er et sett regler som gjelder for alle EU/EØS-land. Sammen med særlovgivning om personvern på enkelte områder, utgjør dette personvernregelverket.

Loven handler om behandling, innsamling og bruk av personopplysninger. Lovens formål er å sikre vern av fysiske personer i forbindelse med behandling av personopplysninger.

Artikkel 5 nr. 1 fastsetter nærmere angitte grunnkrav (prinsipper) for behandling av personopplysninger. Alle som behandler personopplysninger må opptre i samsvar med disse grunnleggende prinsippene:

1. Personopplysninger skal

a) behandles *lovlig, rettferdig og gjennomsiktig*
b) samles inn for spesifikke, uttrykkelige angitte og berettigende formål (formålsbegrensning)
c) være adekvate, relevante og begrenset til det som er nødvendig (dataminimering)
d) være korrekte og nødvendig oppdaterte (riktighet)
e) lagres slik at det ikke er mulig å identifisere de registrerte lengre enn nødvendig (lagringsbegrensning)
f) behandles på en måte som sikrer tilstrekkelig beskyttelse mot uberettiget innsyn og endringer ved bruk av egnede tekniske eller organisatoriske tiltak (integritet og konfidensialitet)

2. Den behandlingsansvarlige er ansvarlig for og skal kunne påvise at nr. 1 overholdes (*ansvarlighet)*

Fylkeskommunen som skoleeier og skolene må oppfylle grunnkravene for å kunne behandle personopplysninger. Dersom grunnkravene ikke er oppfylt vil dette gi et svekket personvern for elevene i skolen. Grunnkravet i bokstav f ovenfor, integritet og konfidensialitet (fortrolighet), er spesielt relevant for vårt tema.

Integritet handler om at informasjon som behandles i IKT-systemene ikke skal kunne endres utilsiktet eller uautorisert. Skoleeier og skolene skal ha et bevisst forhold til hvem som skal ha adgang til å endre informasjon som er lagret i ulike systemer. Konfidensialitet betyr at skoleeier og skolene skal sørge for at bare de som trenger tilgang til personopplysningene får tilgang til dem. Skoleeier skal med andre ord ha et bevisst forhold til hvem som får og hvem som ikke får tilgang (autorisasjon) til systemer som inneholder personopplysninger, og hvilken informasjon det blir gitt tilgang til. Dette kalles tilgangsstyring. Jo mer sensitive personopplysningene er, jo bedre skal de sikres i forhold til konfidensialitet og integritet. Tiltak som sikrer konfidensialitet og integritet er å beskytte tilgang til personopplysninger med autentisering, og sikre at det kun er ansatte med behov for tilgang som får tilgang.

Den behandlingsansvarlige er den som er overordnet ansvarlig for å overholde personvernprinsippene og regelverket. I dette prosjektet vil det være Innlandet fylkeskommune som er den behandlingsansvarlige. Ansvaret til den behandlingsansvarlige utdypes i artikkel 24, hvor det fastsettes en forpliktelse til å gjennomføre «egnede tekniske og organisatoriske tiltak», jf. artikkel 24 nr. 1. Tiltakene skal både «sikre» og «påvise» at behandlingen utføres i samsvar med forordningens regler.

3.1.2 KOMMUNELOVEN KAPITTEL 25

Internkontrollen etter kommuneloven kapittel 25 gjelder administrasjonens virksomhet og omfatter alt som er innenfor ansvarsområdet til kommunedirektøren.

Internkontroll innebærer ifølge kommuneloven § 25-1:

a. En beskrivelse av virksomhetens hovedoppgaver, mål og organisering.
b. Nødvendige rutiner og prosedyrer.
c. Avdekke og følge opp avvik og risiko for avvik.
d. Dokumentere internkontrollen i den formen og det omfanget som er nødvendig.
e. Evaluere og ved behov forbedre skriftlige prosedyrer og andre tiltak for internkontroll.

Etter bokstav d) skal internkontrollen dokumenteres i den formen og det omfanget som er nødvendig. KS har utarbeidet en veileder til kommuneloven kapittel 25 "Orden i eget hus". Veilederen beskriver at det vil være opp til kommunen (kommunedirektøren) å avgjøre hva som er nødvendig å dokumentere, men det er opplagt at kravet gjelder både rutiner og prosedyrer, risikoanalyser, iverksatte tiltak og avvikshåndtering m.m. Kravet om dokumentasjon av internkontrollen bør videre ses i sammenheng med kravet i b) om at det skal etableres

nødvendige rutiner og prosedyrer, og pålegget i e) om å evaluere og ved behov forbedre skriftlige prosedyrer og andre tiltak for internkontroll.[9]

3.1.3 FYLKESKOMMUNENS STYRINGSDOKUMENTER

Fylkeskommunen har utarbeidet et styringsdokument for personvern og informasjonssikkerhet som er godkjent 07.04.2021.[10] I styringsdokument for personvern og informasjonssikkerhet er det satt opp noen grunnleggende prinsipper for hvordan Innlandet fylkeskommune skal ivareta informasjonssikkerheten. Ett av prinsippene sier at *all tilgang til personopplysninger og systemer skal baseres på tjenstlig behov, og skal ivareta god ansvarsfordeling*. Ett annet sier at *arbeidet med informasjonssikkerhet skal være risikobasert.*

Det er også satt opp en rekke krav til personvern og informasjonssikkerhet som skal ivaretas. Det skal blant annet gjennomføres risikovurderinger jevnlig og ved endringer som kan påvirke risikobildet, samt iverksettes sikkerhetstiltak for å sikre et akseptabelt risikonivå. Videre er det satt krav til å etablere, teste og vedlikeholde planer og systemer, samt til å rapportere og håndtere avvik og uønskede hendelser. Arbeidet med personvern og informasjonssikkerhet skal være basert på anerkjente standarder og veiledninger, blant annet ISO 27000-serien og Datatilsynets veiledninger om personvern.

Det er utarbeidet et dokument med overordnede Arkitekturprinsipper for Innlandet fylkeskommune, dette er styringsprinsipper for valg av løsninger i forbindelse med innføring, utvikling og forvaltning av fylkeskommunens digitale tjenester. Prinsipp 4 i dokumentet omhandler informasjonssikkerhet og personvern, og innebærer at *all informasjon skal sikres og beskyttes mot brudd på konfidensialitet, integritet og tilgjengelighet ut fra en risikobasert tilnærming.*

Revisor legger etter dette til grunn at tilgang til IKT-systemer skal være i henhold til tjenstlig behov og at informasjonen i systemene skal sikres mot at uvedkommende får tilgang, basert på en risikobasert tilnærming.

3.1.4 ANERKJENTE STANDARDER OG VEILEDNING

Ifølge fylkeskommunens styringsdokument for personvern og informasjonssikkerhet baserer de arbeidet med personvern blant annet på datatilsynets veiledninger. Datatilsynet har utarbeidet en oversikt over alle plikter virksomheten har etter personvernregelverket.

Datatilsynet beskriver at personopplysninger skal behandles slik at opplysningenes integritet, konfidensialitet og tilgjengelighet beskyttes. Dette betyr at personopplysningene må sikres mot uautorisert tilgang. Misbruk av passord og brukernavn er ofte den raskeste og enkleste veien inn til virksomhetens nettverk og informasjonssystem, eller for å få tilgang til virksomhetens personopplysninger. For å unngå dette er det viktig med god håndtering av passord.

---

[9] https://www.ks.no/globalassets/fagomrader/lokaldemokrati/internkontroll/Kommunedirektorens-internkontroll-veileder-08092020.pdf

[10] Styringsdokument for personvern og informasjonssikkerhet, godkjent av administrasjonssjefen.)

Datatilsynet anbefaler sterk autentisering (tofaktorautentisering/totrinnsbekreftelse/flerfaktorautentisering) ved behandling av sensitive personopplysninger da dette gir bedre beskyttelse enn passord alene. Derfor skal bruk av sterk autentisering vurderes som et av sikkerhetstiltakene. Et typisk eksempel på hvor det vil kreves sterk autentisering er når en person har tilgang til et informasjonssystem med sensitive personopplysninger og/eller personopplysninger om mange over eksterne nett som er utenfor virksomhetens kontroll.[11]

Ifølge fylkeskommunens styringsdokument for personvern og informasjonssikkerhet baserer de arbeidet med personvern også på ISO 27000 serien. ISO 27001 er en internasjonal standard som er utarbeidet for å stille krav til etablering, implementering, vedlikehold og kontinuerlig forbedring av et ledelsessystem for informasjonssikkerhet (internkontroll for informasjonssikkerhet).[12]

Krav til å utarbeide overordnet retningslinje for tilgangskontroll fremgår av vedlegg A punkt. 9.1.1 i ISO 27001.
I henhold til punkt 6.1.3 *Håndtering av informasjonssikkerhetsrisikoene* skal virksomheten fastsette alle sikringstiltak som er nødvendige for å håndtere risiko knyttet til informasjonssikkerhet. Tillegg A inneholder en omfattende liste over sikringstiltak som skal brukes i sammenheng med punkt 6.1.3. Ett av punktene i vedlegg A (A.9) omhandler tilgangsstyring (aksesskontroll) og hovedtrekkene blir kort gjengitt nedenfor:

- Brukere skal bare gis tilgang til nettverk og nettjenester som de er spesifikt autoriserte til å benytte – tjenstlig behov.
- Det skal implementeres en formell prosess for registrering og sletting av brukere som gis tilgangsrettigheter.
- Det skal implementeres en formell prosess for forvaltning av brukertilganger, herunder for å tildele eller inndra tilgangsrettigheter for alle typer brukere i alle systemer og tjenester.
- Brukernes tilgangsrettigheter skal gjennomgås ved jevne mellomrom.
- Tilgangsrettigheter skal fjernes ved opphør av arbeidsforhold, kontrakt eller avtale, eller korrigeres ved endringer.
- Der det er påkrevd av policyen for tilgangskontroll skal tilgang til systemer og applikasjoner kontrolleres gjennom en sikker påloggingsprosedyre, basert på risiko.
- Det skal være et styringssystem for passord.

Informasjonsklassifisering er helt sentralt i informasjonssikkerhet ettersom det blir benyttet for å klassifisere informasjon og IT-systemer i ulike sikkerhetsklasser, jf. ISO 27001 A.8.2. Klassifiseringen brukes til å sette sikkerhetsnivå på system, f.eks. vil system som håndterer strengt fortrolige data være underlagt et strengere sikkerhetsregime, og dermed strengere tilgangsstyring, enn et system som bare har åpne data. Det er vanlig å vurdere informasjonen i systemet opp mot viktigheten av å ivareta konfidensialitet, integritet og tilgjengelighet.

Nasjonal sikkerhetsmyndighet (NSM)[13] har utarbeidet et sett med grunnprinsipper og anbefalte tiltak for å beskytte informasjonssystemer mot uautorisert tilgang, skade og misbruk. NSMs grunnprinsipper for IKT-

[11] https://www.datatilsynet.no/rettigheter-og-plikter/virksomhetenes-plikter/informasjonssikkerhet-internkontroll/passordanbefalinger/
[12] Informasjonsteknologi Sikringssystemer Ledelsessystemer for informasjonssikkerhet. Krav. (ISO/IEC 27001:2013 innebefattet Cor 1:2014 og Cor 2:2015.ddd
[13] Nasjonal sikkerhetsmyndighet (NSM) er fagorgan for forebyggende sikkerhet, og sikkerhetsmyndighet etter lov om nasjonal sikkerhet (sikkerhetsloven). https://nsm.no.

sikkerhet er et supplement til eksisterende nasjonale og internasjonale regelverk, standarder og rammeverk innen IKT-sikkerhet.

Grunnprinsipp 1.3 *Kartlegg brukere og behov for tilgang* har som mål at virksomheten skal ha oversikt over hvilke brukergrupper, brukere og tilgangsbehov som finnes i virksomheten og ha kartlagt ansvar for IKT-sikkerhet. Grunnprinsipp 2.6 *Ha kontroll på identiteter og tilganger er* spesielt relevant i dette prosjektet. Målet med prinsippet er at virksomheten skal ha oversikt over identiteter og kontoer i informasjonssystemene og styre tilgang til ressurser effektivt og i henhold til virksomhetens retningslinjer.

Nedenfor omtaler vi noen anbefalte tiltak for at virksomheten skal oppnå kontroll på identiteter og tilganger:

- *Etabler retningslinjer for tilgangskontroll:* Retningslinjen bør følge minste privilegiums prinsipp ved at brukerkontoer ikke får flere privilegier (tilgangsrettigheter) enn nødvendig. Alle kontoer bør kunne spores til en ansvarlig bruker og alle kontoer bør kunne spores til en ansvarlig rolle og person som godkjente dette. Kontoer, tilganger og rettigheter bør revideres jevnlig. Dette er spesielt kritisk mht. kontoer, tilganger og rettigheter for drift og spesialbrukere. Gjenbruk identiteter mest mulig på tvers av systemer, delsystemer og applikasjoner (ideelt «Single sign on»).

- *Etabler en formell prosess for administrasjon av kontoer, tilganger og rettigheter:* Prosessen bør omfatte hele livssyklusen og omfatte opprettelse, vedlikehold og deaktivering. NSM anbefaler å deaktivere fremfor å slette kontoer og tilganger slik at revisjonsspor bevares, i henhold til gjeldende lover og regelverk. Retningslinjer for tilgangskontroll og prosess for administrasjon av kontoer, tilganger og rettigheter bør dokumenteres og være kjent i virksomheten.

- *Minimer rettigheter til sluttbrukere og spesialbrukere:* Ikke tildel administrator-rettigheter til sluttbrukere. Oppgavene bør skilles i to kontoer. En for vanlig kontorbruk som e-post og internett-søk og en annen for oppgaver som krever forhøyet rettigheter. Disse kontoene bør ha tilstrekkelig sikkerhetsskille og som absolutt minimum ikke ha samme passord.

- *Bruk flerfaktor autentisering for å autentisere brukere:* Implementer som et minimum multi-faktor på brukerkontoer som har tilgang til kritiske data eller systemer, samt brukere med driftsoppgaver. Der multi-faktor autentisering ikke støttes, bør brukerkontoer bli pålagt å bruke sterke passord på systemet.

Mangelfull sikkerhetsovervåking i informasjonssystemer, samt mangelfull sammenstilling og analyse av sikkerhetsrelevante data gjør at angripere kan skjule tilstedeværelse, handlinger og aktiviteter i virksomhetens informasjonssystemer, jf. NSMs grunnprinsipp 3.2 *Etabler sikkerhetsovervåking.* Dette prinsippet er sentralt i sammenheng med tilgangsstyring. Selv om en virksomhet vet at systemer og maskiner har blitt infiltrert, kan de ikke se detaljene i hendelsen dersom virksomheten ikke har etablert tilstrekkelig sikkerhetsovervåking.

For å etablere sikkerhetsovervåking knyttet til tilgangskontroll anbefaler NSM at man som minimum bør samle inn data knyttet til vellykkede og mislykkede påloggingen på enheter og tjenester. Videre samle administrasjons- og sikkerhetslogger fra enheter og tjenester i IKT-systemene. For klienter bør man i tillegg som minimum registrere forsøk på kjøring av ukjent programvare og forsøk på å få forhøyede systemrettigheter («privilege escalation»).

3.1.5 KONKRETE REVISJONSKRITERIER

Med bakgrunn i relevant lovverk, fylkeskommunens styringsdokumenter og anerkjente standarder og veiledninger har revisjonen utarbeidet konkrete revisjonskriterier som fylkeskommunens praksis måles opp mot. De konkrete revisjonskriteriene blir presentert for hver av problemstillingene nedenfor.

Problemstilling 2:
I hvilken grad er det etablert grunnleggende retningslinjer og rutiner for tilgangsstyring i IKT-systemer som behandler elevdokumentasjon?

1. Fylkeskommunen bør ha en overordnet retningslinje eller policy for tilgangsstyring som en del av styringssystemet for informasjonssikkerhet. Denne bør inneholde:
    a. Rutiner for tildeling, endring, sletting og kontroll av tilganger.
    b. Rutiner for autentisering basert på graden av sensitivitet i opplysningene og hvilken enhet pålogging skjer fra.
    c. Ansvarsfordeling innen tilgangskontrollen.

2. Fylkeskommunens retningslinjer og rutiner/policy for tilgangsstyring bør være basert på en overordnet informasjonsklassifisering som klassifiserer informasjon med hensyn til behov for konfidensialitet, integritet og tilgjengelighet, og som styrer systemenes sikkerhetsnivå.

3. Fylkeskommunen bør ha et system for brukeridentiteter og passord, all tildeling av rettigheter til tilgang bør registreres i et register.

4. Fylkeskommunen bør ha etablert sikkerhetsovervåking for å avdekke sikkerhetshendelser relatert til tilgangskontrollen.

Problemstilling 3:

I hvilken grad er det etablert rutiner og praksis for kontroll av tilgangsstyringen i utvalgte IKT-systemer som behandler personopplysninger om elever i videregående opplæring?

1. Tilgangsstyringen i IKT-systemet bør være innrettet i henhold til risikovurdering av informasjonsverdiene i systemet.

2. Fylkeskommunen bør ha implementert en formell prosess for å registrere brukere som gis tilgangsrettigheter og for forvaltning av brukertilganger i IKT-systemet. Prosessen bør omfatte hele livssyklusen til en brukerkonto. Retningslinje for tilgangskontroll og prosess for administrasjon av kontoer, tilganger og rettigheter bør dokumenteres og være kjent i virksomheten.

3. Tilgang til IKT-systemer skal være basert på tjenstlig behov.

4. Fylkeskommunen bør ha oversikt over hvem som har tilgang til de utvalgte IKT-systemene og hvem som har gitt tilgang.

5. Fylkeskommunen bør ha et system for jevnlig kontroll og gjennomgang av om tildelte tilganger i IKT-systemet er korrekte.

6. Fylkeskommunen bør ha kontroll på service-/systemkontoer, utviklere og driftsbrukere og hvilke rettigheter disse kontoene har. Det bør ikke tildeles administratorrettigheter til sluttbrukere.

7. IKT-systemets bruker- og administratorkontoer som forvalter sensitive personopplysninger, bør være beskyttet av sterk autentisering.

4 FAKTABESKRIVELSE OG VURDERINGER

I dette kapittelet beskriver vi innsamlede data for hver av de tre problemstillingene. For problemstilling to og tre utgjør faktabeskrivelsen grunnlaget for våre vurderinger opp mot revisjonskriteriene vi utledet i kapittel 3. Fakta og vurderinger behandles for den enkelte problemstilling under hvert delkapittel.

4.1 IKT-SYSTEMER SOM BEHANDLER ELEVDOKUMENTASJON

Dette delkapittelet svarer på problemstilling 1:

> Hvilke IKT-systemer behandler personopplysninger om elever i videregående opplæring, og hvilke personopplysninger behandles i de ulike IKT- systemene?

Delkapittelet beskriver IKT-systemene som behandler elevdokumentasjon i videregående opplæring i Innlandet fylkeskommune. Det er ikke utledet revisjonskriterier til denne problemstillingen.

Fylkeskommunen gjorde vinteren 2021 en kartlegging av alle IKT-systemer og applikasjoner som benyttes ved de videregående skolene i Innlandet. Ifølge kartleggingen er det omtrent 150 systemer eller applikasjoner som behandler personopplysninger om elever i skolene. Antallet endres over tid da noen verktøy fases ut, og nye kommer til. Dette er digitale læremidler, pedagogiske læremidler og andre programmer/nettbaserte tjenester som krever at bruker logger på, men hvor det er svært begrenset med personopplysninger som lagres. Revisjonen har valgt å avgrense fremstillingen til større IKT-systemer der elevdokumentasjon registreres og behandles.

Revisjonen har fått oversendt dokumentasjon fra fylkeskommunen som beskriver hvilke IKT-systemer som behandler elevdokumentasjon i videregående opplæring, og hvilke personopplysninger som behandles i de ulike systemene.

Fra og med skolestart høsten 2021 ble det endringer i fylkeskommunens bruk av IKT-systemer i videregående skole. Læringsplattformene ItsLearning og Fronter ble faset ut og er ikke lenger i bruk. Systemene er erstattet med Microsoft Teams for Education. Videre skal det ikke lagres elevdokumentasjon i læreres filstruktur på PC fra skolestart høsten 2021. Lagring skal ifølge fylkeskommunen kun skje i fagsystemer, Elements eller Microsoft Teams for Education med tilgangsstyring basert på tjenstlig behov. IKT-systemene som fra høsten 2021 ikke benyttes av fylkeskommunen, herunder ItsLearning og Fronter, omtales ikke i rapporten.

4.1.1 VIGO

Om systemet
VIGO er fellesbetegnelsen på et IKT-system som inneholder flere «moduler». Disse modulene inneholder program som i en eller annen form håndterer informasjon om elever i videregående opplæring. Det er 11 fylkeskommuner og Oslo kommune i fellesskap som eier og finansierer utviklingen av systemet. Forvaltningen foretas av Vigo Interkommunale Selskap.

VIGO er et inntaks- og administrasjonssystem som benyttes av inntaks- og fagopplæringsavdelingene, oppfølgingstjenesten, opplæringskontor, lærebedrifter og ansatte på de videregående skolene i fylkeskommunen. Systemet inneholder:

- Et søkesystem for inntak til videregående opplæring/voksenopplæring/fagskole
- Et inntakssystem til videregående opplæring/fagskole
- Et system for formidling av lærlinger/lærekandidater til bedriftene
- Et system for beregning av tilskudd til bedrifter som har lærlinger/lærekandidater
- En sentral database med informasjon om videregående opplæring
- Et system for leveranse av kvalitetssikret data til internt og eksternt bruk
- Et system for leveranse av kodeverk til eksterne samarbeidspartnere
- Et system til bruk for oppfølgingstjenesten

Søknad om skoleplass er tilgjengelig for elever fra januar og fylles ut med ønsker fra elever frem til 1. mars. Inntak behandles av Inntakskontoret i IFK i juli og august. I midten av august overføres opplysningene til skolene fra VIGO til Visma in School. Søknadene for hvert år beholdes frem til 1. november, da overføres all søkerinformasjon til elevmappe i Vigo. Opplysningene som lagres i elevmappen er personalia, historiske søknader, hva man har gått og når, kompetansebevis, skole, om man har søkt skole i andre fylker og om man har vært registrert hos OT.

Personopplysninger som behandles i VIGO

Opplysninger som behandles i VIGO er navn, kontaktinformasjon, personnummer, fag, karakterer, fravær, skoletilknytning, bedriftsopplysninger, elevens rettsforbruk, morsmål, oppholdstillatelse, nasjonalitet med mer. I tillegg lagres informasjon fra grunnskole, inntakspoeng og fremmedspråk.

Hvem har tilgang til VIGO?
VIGO brukes hovedsakelig sentralt i fylkeskommunen ved inntakskontoret. På skolene har noen få ansatte lesetilgang til søkere til egen skole, og etter at inntaket er gjennomført har de lesetilgang til informasjon om elevenes karakterer og fravær fra forrige skoleår. Brukertilganger blir tildelt og vedlikeholdt av systemansvarlig for VIGO (to personer) i henhold til brukers behov.

4.1.2 VISMA INSCHOOL

Om systemet

Visma InSchool (VIS) leveres av Visma og er et skoleadministrativt system. Systemet benyttes til administrasjon av personalopplysninger, administrasjon av eksterne vikarer, administrasjon av foresatt opplysninger[14] og elevtilknytning, samt administrasjon av elevopplysninger, herunder elevadministrasjon, oppfølging av elever og oppfølging av elever med særskilte opplæringsløp. Systemet ble innført i alle videregående skoler i Innlandet fylkeskommune høsten 2020. Systemet er fortsatt under utvikling og ny funksjonalitet vil bli utviklet innenfor flere områder.

Personopplysninger som behandles i Visma InSchool

Systemet behandler følgende personopplysninger om elever:

- Personalia (navn, fødselsnummer, kjønn, adresse, telefon, e-postadresser og fødselsdato)
- Utdanningsinformasjon (klasser/fag den enkelte elev tar, undervisningsgruppetilknytning, utdanningshistorikk og slutt/start-dato)
- All informasjon som danner grunnlag for elevens vitnemål, som vurderinger, karakterer og fravær
- Bilde av elev
- Informasjon om foresatte (navn, fødselsnummer, adresse, telefon og e-postadresser)

IFK opplyser at Visma InSchool (VIS) er det eneste skoleadministrative IKT-systemet som blir benyttet av skolene. Dette systemet skal innen høsten 2023 brukes av alle VGS i landet. Ifølge retningslinjer som er kommunisert ut til skolene så skal all vurdering som danner grunnlag for elevenes vitnemål lagres i dette systemet for å sikre at all dokumentasjon er på én plass. VIS skal etter hvert få et eget innleveringsverktøy, tentativt høsten 2022. Man kjenner ikke fullstendig funksjonalitet før dette er klart.

Hvem har tilgang til Visma InSchool

Brukere av VIS er ansatte med tjenstlig behov i videregående skole, hos skoleeier og i ulike støtteavdelinger i fylkeskommunen, som HR/lønn og arkiv. Tilgangsrettigheter til VIS blir styrt automatisk ut fra hvilken rolle man har. En lærer har for eksempel bare tilgang til elever som han/hun er registrert som lærer for. I tillegg kan man få utvidede tilganger til systemer, ved at det legges ekstra tilganger til en rolle, f.eks. dersom man jobber i administrasjonen.

Tilganger i VIS er på flere nivåer; lærertilgang, elevtilgang, foresatt-tilgang og basistilgang ut fra hva den enkelte har behov for. Kontaktlærere har utvidet tilgang og kan se vurderinger for alle elever i sin klasse. Faglærere ser kun de elevene han/hun har i sitt fag. Tilgangene til systemet faller automatisk bort når ansatte slutter. Elevene mister tilgang til systemet når man bytter til nytt skoleår i VIS. Elevene får tilgang igjen første skoledag. Ansatte som er tilsatt over flere skoleår vil ligge med samme tilganger, og vil ha tilgang til VIS også ved overgang mellom skoleår.

[14] Det er fortrinnsvis informasjon om foresatte for elever under 18 år som behandles i systemet. Foresatte slettes automatisk fra løsningen så snart elevene fyller 18 år. Det kreves eget samtykke fra både elev og foresatt dersom foresatt-opplysninger skal lagres etter at eleven er fylt 18 år.

4.1.3 CONEXUS ENGAGE OG OPPFØLGINGSLOGGEN

Om systemene
Engage og Oppfølgingsloggen er to adskilte IKT-systemer fra samme leverandør som brukes i det systematiske arbeidet med frafallsforebygging etter IKO-modellen. Systemene blir beskrevet i samme delkapittel da de henger naturlig sammen i arbeidet med frafallsforebygging i videregående skole.

Engage og Oppfølgingsloggen leveres av firmaet Conexus. Det var opprinnelig Oppland, Hedmark, Akershus, Aust-Agder og Nord Trøndelag fylkeskommuner som anskaffet systemene knyttet til et felles prosjekt for å jobbe med å redusere frafall i videregående skole etter IKO-modellen[15].

IKO-modellen skal bidra til at skolen raskt kan identifisere elever med høy risiko for å falle fra og løpende kartlegging skal bidra til rask iverksettelse av støttetiltak for eleven. Gjennom det systematiske identifiserings- og kartleggingsarbeidet vil læreren få klarhet i årsaken til at den enkelte elev eventuelt står i fare for å ikke fullføre videregående opplæring. Skolen skal bruke kartleggingen til å definere en oppfølging med mål om at eleven raskest mulig skal få fullt utbytte av den ordinære opplæringen. For å systematisere og kvalitetssikre identifiseringen, kartleggingen og oppfølgingen benyttes Engage og Oppfølgingsloggen.

Engage er «grunnmodulen» der det avdekkes hvem som kan stå i faresonen for å slutte på skolen. Det var i februar 2021 registrert 13 551 elever i systemet og 3 827 ansatte som hadde tilgang til systemet.

Oppfølgingsloggen følger opp bekymringsmeldinger om elever som er i fare for å droppe ut av skolen, bekymringsmeldingene sendes fra Engage. Oppfølgingsloggen har et sikkerhetsnivå som gjør det mulig å behandle særlige kategorier personopplysninger (nivå 4). I Oppfølgingsloggen registreres koder som angir elevens hovedutfordringer, det settes opp en plan med tiltak, hvem som har ansvar for gjennomføring og tidsramme for tiltakene, samt evaluering av effekten av tiltakene. Oppfølgingsloggen skal sikre systematikk og oversikt i oppfølgingen slik at eleven får tilpasset opplæring eller andre tiltak som reduserer risikoen for frafall. I Oppfølgingsloggen fremkommer det tydelig hvem som har oppfølgingsansvaret, og det er bare ansvarlig for tiltaket som får tilgang til å se opplysningene. Dette er som oftest kontaktlæreren. Ansvar for selve gjennomføringen av tiltakene avhenger av utfordringens art, og kan være knyttet til f.eks. en faglærer, sosialrådgiver, eller elevtjenesten.[16]

Personopplysninger som behandles
Engage behandler personopplysninger om elever i form av navn, fødselsnummer, kjønn, fravær og karakterer.

I Oppfølgingsloggen er det mulig å lagre eventuelle kartlegginger av elevens faglige ståsted, generelle utfordringer eleven har, tiltakstyper, møter, samtaletidspunkt og notater relatert til oppfølging av eleven. Referat fra samtale med eleven rundt faglige og sosiale utfordringer lagres ikke i Engage, men logging av gjennomføring av tiltak skjer i Oppfølgingsloggen. I Oppfølgingsloggen finnes det mulighet til å «kode» «helseutfordringer» eller «sosiale forhold» og det kan i noen tilfeller bli registrert særlige kategorier personopplysninger i fritekstfelt.

---

[15] *IKO står for identifisering, kartlegging og oppfølging.*

[16] Fra dokumentet «Tidlig innsats når det gjelder, IKO – en modell for systematisk frafallsforebygging»

Hvem har tilgang
Brukere av systemene er faglærere, kontaktlærere, IKO-ansvarlige, rådgivere (elevtjenesten), skoleadministrator av Engage, skoleledere (rektor og avdelingsledere) og IKO-ansvarlig i sentraladministrasjonen. Tilgangsstyringen er separat for de to systemene.

I Engage tildeles tilganger i utgangspunktet automatisk med bakgrunn i rolle og relasjoner i Visma InSchool. Tilganger kan også tildeles manuelt av skoleadministrator. Hver skole er ansvarlig for å vedlikeholde sine tilganger. Som «default» er det ingen ansatte som får tilganger med mindre det skoleadministrative systemet gir opplysninger som forteller hvilke klasser den ansatte skal være tilknyttet.

I Oppfølgingsloggen tildeles tilganger manuelt av skoleadministrator per sak. Oppfølgingsloggen har ingen automatisk tilgangstildeling.

4.1.4 ELEMENTS

Om systemet
Elements er fylkeskommunens elektroniske sak- og arkivsystem. Systemet leveres av Sikri som en offentlig skyløsning[17] og benyttes av alle fylkeskommunens enheter. Alle elever ved videregående skoler i Innlandet har sin egen elevmappe i Elements.

Personopplysninger som behandles i Elements

I Elements lagres fylkeskommunens personalmapper, elev/utdanningsmapper, politiske saker, anskaffelser og dokumenter knyttet til generell saksbehandling. I tillegg til elev/utdanningsmapper registreres det også andre opplysninger om elever, eksempelvis saker om mobbing/skolemiljøsaker eller rus. I disse tilfellene registreres det en egen sak på dette i Elements.

Hvem har tilgang til Elements
Bare personer med tjenstlig behov skal ha tilgang til taushetsbelagte opplysninger i elektronisk arkiv i Elements. Innsyn i opplysninger begrenses ved at brukere tildeles roller og tilgangskoder i systemet. Ansattes personalleder skal tildele tilganger i henhold til ansattes ansvarsområde og oppgaver, dvs. leder autoriserer ansatte til å få tilgang til nødvendig informasjon etter tjenstlig behov.

Det er definert fire ulike roller for tilgang i Elements; *leder, saksbehandler, sekretær og arkivar*. Ulike roller gir tilgang til ulike funksjoner i systemet, f.eks. journalføre dokumenter, fordele post og godkjenne dokumenter.

Det er kun ansatte med tjenstlig behov som gis tilgang til elev-/utdanningsmappene. Det betyr at det kun er ansatte som har opplærings-/oppfølgingsansvar for eleven, jf. opplæringsloven og annen lovgivning, som har tilgang. Dette gjelder ansatte ved alle de videregående skolene og ansatte ved avdelingen Kompetanse og tannhelse.

Følgende grupper har tilgang til å lese dokumenter i elev-/utdanningsmapper ved egen avdeling/skole:

- Rektorer, ass. rektorer, avdelingsledere

[17] I en offentlig sky er det ekstern leverandør som er vert og vedlikeholder IT-løsningen.

- Rådgivere: Utdannings- og yrkesrådgivere, sosialpedagogiske rådgivere og helserådgivere (Oppland), OT-veiledere (Oppfølgingstjenesten)
- Merkantilt ansatte

Rådgivere har tilgang til Elements da de håndterer viktig elevdokumentasjon som eksempelvis referater fra samtaler og kartlegginger som skal arkiveres i Elements.

Lærere skal normalt ikke ha direkte tilgang til Elements, men lærere i videregående skoler i tidligere Oppland får tilgang til elevdokumentasjon ved bruk av LAO-løsningen (Lærerens arbeidsoppgaver). Lærere i videregående skoler i tidligere Hedmark kan få tilgang til aktuelle utdanningsmapper enten via avdelingsledere eller etablerte interne rutiner for oppslag i Elements.

4.1.5 MICROSOFT OFFICE 365

Om systemet
Microsoft Office 365 inneholder tradisjonelle kontorstøtteapplikasjoner som Word, Excel, og PowerPoint. Microsoft Office 365 er skybasert og man får også tilgang til skytjenester for deling og samarbeid. Microsoft Exchange sørger for e-post, kalendre og booking av møter. SharePoint organiserer ansattes dokumenter i biblioteker, og i One Drive for business og OneNote kan man lagre og dele dokumenter. Microsoft Teams forener mye av denne funksjonaliteten og gir i tillegg en chatbasert plattform for samhandling og kommunikasjon.

Vi vil i det følgende presentere Teams for Education, OneNote og OneDrive nærmere da det er disse programmene i Microsoft Office 365 som brukes til lagring og formidling av elevdokumentasjon.

Teams for Education benyttes som en læringsplattform i undervisning og samhandling med elever. Teams har en funksjonalitet for videomøter, samt en funksjon som kalles klasseteam. Klasseteam har oppgaveverktøy der elever kan få utdelt og levere inn oppgaver. Klasseteam har i tillegg en funksjon som heter klassenotatblokk, dette er en OneNote med spesiell funksjonalitet og tilgangsstyring. Klassenotatblokk er en form for elektronisk ringperm som gjør det mulig å samle informasjon og læringsmateriell. Elever kan levere oppgaver i klassenotatblokk og oppgavemodul i Teams.

OneNote brukes også til deling av ressurser mellom lærere. Det kan brukes til deling av ressurser med elever, men det er ikke anbefalt. Elever bruker OneNote til lagring av eget skolearbeid og til deling av ressurser med lærer.

OneDrive brukes av lærere til å lagre undervisningsdokumenter, til lagring av elevbesvarelser som lastes inn på egen PC (skal fjernes etter retting), og til mellomlagring av arbeidsdokumenter som referater, notater om elver og lignende. OneDrive brukes av lærere til å lagre undervisningsopplegg til elever (klassenotatblokk), møtereferater og arbeidsnotater. Elever bruker OneDrive til å lagre notater og til besvarelser i ulike fag (klassenotatblokk).

Personopplysninger som lagres
I Teams for Education lagres innleveringer, prøver, vurderinger og kommunikasjon mellom lærer og elev.

Lærernes personlige notater og arbeidsdokumenter lagres i OneDrive eller OneNote. Innlandet fylkeskommune har gitt skolene retningslinjer om at ingenting skal lagres lokalt på egen PC. Det er gitt føringer på at

undervisningsopplegg skal lagres på OneDrive eller egen OneNote. Undervisningsopplegget deles med elever i Teams for Education.

For møtereferater og opplysninger om elever, eksempelvis referat fra klasseråd og notater om enkeltelever skal filene krypteres og lagres på OneDrive.

Hvem har tilgang til Teams for Education, OneNote og OneDrive
Det skal kun være tilgang til disse opplysningene etter tjenstlig behov. Det er gitt retningslinjer om at dokumentene ikke skal skrives ut og skal kun sendes via e-post dersom dokumentet er kryptert.

4.1.6 LAO

Om systemet
LAO (Lærerens administrative oppgaver) er et IKT-system som digitaliserer arbeidsprosessen med å skrive varsel til elever i fag, atferd, orden, og varsel om vedtak. Videre brukes det til å skrive vedtak, IOP[18], halvårsrapport og årsrapport om spesialundervisning. LAO skal bidra til å kvalitetssikre innholdet i hver prosess i spesialundervisningen, fra sakkyndig vurdering er utarbeidet til årsrapporten foreligger.
LAO kommuniserer med Visma InSchool, fylkeskommunens skoleadministrative system. Vedtak ompesialundervisning og andre dokumenter som skrives i LAO journalføres automatisk i elevens mappe i Elements. Dokumentet blir i samme prosess sendt til KS SvarUt,[19] der dokumentet automatisk blir sendt ut til elev/foreldre.

Det foreligger et reservasjonsregister for LAO som skal sikre at dokumenter ikke sendes til foreldre der foreldre ikke skal ha informasjon om eleven, eller om det er elever med hemmelig adresse. I tilfeller der elev er registrert i reservasjonsregisteret vil det oppstå en automatisk feil i forsendelsen og dokumentet må manuelt arkiveres i Elements av IKT. Videre får aktuell skole beskjed om at dokumentet må sendes rette vedkommende.

Alle videregående skoler i tidligere Oppland bruker LAO varsel, ingen skoler i tidligere Hedmark gjør dette. Alle videregående skoler i tidligere Oppland, med unntak av Gjøvik VGS og Hadeland VGS bruker LAO Spesialundervisning, ingen i tidligere Hedmark.

I 2020 ble det arkivert 7987 dokumenter i Elements fra LAO, og nesten 1000 i januar 2021.

Personopplysninger som behandles i LAO

I LAO behandles informasjon om elever med spesielle opplæringsbehov som er unntatt offentlighet, samt navn, fødselsdato, fødselsnummer, klasser, fag, faglærere, og kontaktlærer i inneværende skoleår.

Hvem har tilgang til LAO
Faglærere, kontaktlærere, rådgiver, avdelingsleder for spesialundervisning og rektor har tilgang til LAO. Hvilke dokumenter og oppgaver de får tilgang til i LAO er basert på hvilken rolle de er registrert med i fylkeskommunens skoleadministrative system. Lærere får lesetilgang til dokumentasjon vedrørende egne elever, men kun

[18] Individuell opplæringsplan
[19] Sentralisert løsning fra KS som formidler dokumenter mellom avsender og mottaker via ulike kanaler. SvarUt benyttes for utgående post

dokumentasjon som ikke er personsensitiv. Av personsensitive opplysninger får lærer lesetilgang til sakkyndig vurdering for egne elever.

4.2 GRUNNLEGGENDE RETNINGSLINJER FOR TILGANGSSTYRING

I dette delkapittelet svarer vi på problemstilling 2:

> I hvilken grad er det etablert grunnleggende retningslinjer og rutiner for tilgangsstyring i IKT-systemer som behandler elevdokumentasjon?

Problemstillingen undersøker i hvilken grad fylkeskommunen har etablert rutiner og/eller retningslinjer for tilgangsstyring i IKT-systemer som behandler elevdokumentasjon. Problemstillingen tar ikke for seg det enkelte system, men har fokus på om fylkeskommunen har grunnleggende retningslinjer og rutiner på plass for å få til en god tilgangsstyring i IKT-systemene. Informasjonen er basert på samtaler med informasjonssikkerhet- og personvernrådgiver i for Kvalitet, sikkerhet og beredskap, rådgiver i avdeling for IKT og dokumentasjonsforvaltning, samt personvernkoordinator i IFK. Videre har vi innhentet informasjon fra HR om hvordan ansattes brukerkontoer blir opprettet, endret og slettet. Vi har også fått informasjon per e-post fra enhetsleder for Drift og leveranse og enhetsleder for Digitale tjenester i fylkeskommunen.

Til denne problemstillingen har vi utledet følgende revisjonskriterier:

1. Fylkeskommunen bør ha en overordnet retningslinje eller policy for tilgangsstyring som en del av styringssystemet for informasjonssikkerhet. Denne bør inneholde:
    a. Rutiner for tildeling, endring, sletting og kontroll av tilganger.
    b. Rutiner for autentisering basert på graden av sensitivitet i opplysningene og hvilken enhet pålogging skjer fra.
    c. Ansvarsfordeling innen tilgangskontrollen.

2. Fylkeskommunens retningslinjer og rutiner/policy for tilgangsstyring bør være basert på en overordnet informasjonsklassifisering som kategoriserer informasjon innen konfidensialitet, integritet og tilgjengelighet, og som styrer systemenes sikkerhetsnivå.

3. Fylkeskommunen bør ha et system for brukeridentiteter og passord, all tildeling av rettigheter til tilgang bør registreres i et register.

4. Fylkeskommunen skal ha etablert sikkerhetsovervåking for å avdekke sikkerhetshendelser relatert til tilgangskontrollen.

4.2.1 OVERORDNET RETNINGSLINJE FOR TILGANGSSTYRING

Det er seksjon for Kvalitet, sikkerhet og beredskap som har ansvaret for å utarbeide overordnede dokumenter/retningslinjer som omhandler IKT-sikkerhet, deriblant overordnede krav for tilgangsstyring. Ifølge rådgiver i seksjon for Kvalitet, sikkerhet og beredskap skal overordnet retningslinje for tilgangsstyring være en del av fylkeskommunens styringssystem for informasjonssikkerhet. Innlandet fylkeskommune har ingen overordnet retningslinje for tilgangsstyring på tidspunktet revisjonen ble gjennomført, men dette er under arbeid. Retningslinjen skulle være ferdig innen 1. mai 2021, men har blitt utsatt på grunn av kapasitetsproblemer. Retningslinjen er ikke ferdigstilt i perioden forvaltningsrevisjonen har pågått.

Rådgiver i seksjon for Kvalitet, sikkerhet og beredskap opplyser at når overordnet retningslinje for tilgangsstyring er ferdig utarbeidet, skal tjenesteeiere for IKT-systemene i fylkeskommunen lage operative retningslinjer for tilgangsstyring i det enkelte IKT-system.

4.2.1.1 Opprettelse, endring og avslutning av brukerkonto

Med bakgrunn i at fylkeskommunen ikke har en overordnet retningslinje for tilgangsstyring vil revisjonen i det følgene beskrive hvordan brukerkontoer i praksis opprettes, endres og avsluttes. Dette er basert på informasjon fra HR-avdelingen i Innlandet fylkeskommune og oversikt over dataflyt fra enhetsleder for Drift og Leveranse.

Visma HRM er fylkeskommunens mastersystem for lønn og personaladministrasjon. Ved opprettelse av ny brukerkonto overføres automatisk nødvendige ansattopplysninger fra Visma HRM til avdeling for IKT som oppretter en brukerkonto.

Brukerkonto opprettes i praksis ved at ansattopplysningene i Visma HRM blir sendt til MIM (Microsoft identity management)[20]. MIM oppretter bruker og sender automatisk tilbake brukeropplysninger i form av e-post, brukernavn og engangspassord (endres ved første pålogging) til Visma HRM.

Brukerdata i form av brukernavn og passord ligger lagret i katalogsystemet AD (Active Directory)[21] både lokalt hos fylkeskommunen og i sky. En AD-konto (brukerkonto) vil gi vedkommende tilgang til basissystemer som Exchange, Office 365, MinTid, i tillegg til tjenester og systemer som følger den AD-gruppen den ansatte er registrert i. Eksempelvis vil man dersom man jobber som lærer få tilgang til Visma inSchool (skoleadministrativt system) eller andre systemer som det er nødvendig at vedkommende må ha. Dette gjelder kun basistilganger.

Person-, ansatt- og stillingsopplysninger som er opprettet i Visma HRM overføres til Visma inSchool via FINT (integrasjonsløsning)[22]. Fastlønn, variabel lønn og fraværsopplysninger overføres fra Visma inSchool til Visma HRM via FINT.

---

[20] Identitetshåndteringsløsning som bruker persondata fra kildesystemene Visma HRM og VIS og vedlikeholder og synkroniserer disse ut til de tilknyttede systemene. Tanken er at persondata kun skal opprettes og vedlikeholdes ett sted.

[21] Katalogtjeneste i IFK. Satt opp i hybridløsning slik at brukerkontoene i IFK AD blir synkronisert ut til Microsofts skyløsning, Azure.

[22] Felles fylkeskommunale INTegrasjoner. Felles prinsipper og standarder for integrasjoner for fylkeskommuner. FINT forvaltes av Vigo IKS.

Når stillingen eller arbeidsforholdet opphører så sendes det en personalmelding fra ansattes leder. HR avslutter så stillingen /arbeidsforholdet, og alle tilganger opphører. Tilsvarende sendes personalmelding dersom arbeidsforholdet endres.

Brukerkonto til Microsoft-plattform (Office 365) og Feide[23] opprettes automatisk på bakgrunn av registrert informasjon i kildesystemene Visma InSchool og Visma Enterprise HRM. Når en ansatt slutter, blir brukerkontoen deaktivert i tre måneder fra sluttdato. Deretter slettes brukerkontoen med tilhørende filområder og postboks.

Dette er nærmere illustrert i figur 1 som viser dataflyten i Innlandet fylkeskommune.

Figur 1: Unntatt offentlighet, jf. offl. § 24 tredje ledd.

(Avsnitt unntatt offentlighet, jf. offl. § 24 tredje ledd.)

4.2.2 PASSORDSTYRING

Innlandet fylkeskommune benytter Feide og ID-porten for innlogging til systemer som behandler elevdokumentasjon. I tillegg skal det være multifaktor pålogging til Microsoft Office 365. Omtrent alle skole-systemer i Innlandet fylkeskommune bruker Feide, med noen unntak. Dette gjelder blant annet LAO, Conexus Oppfølgingsloggen og VIGO. LAO har autentisering gjennom lokal AD som en lokal applikasjon og ikke via Feide. I Conexus Oppfølgingsloggen og VIGO skjer innloggingen via ID-porten.

Feide
Feide er den nasjonale løsningen for sikker innlogging og datadeling i utdanning og forskning, og leveres av Uninett som samarbeider med Utdanningsdirektoratet og Unit24 om forvaltningen av tjenesten. Feide står for Felles identifikasjon i undervisningen og er en løsning for innlogging til alle skolerelaterte systemer. Svært mange av de digitale læremidlene og tjenestene som er i bruk i norsk utdanning benytter Feide som innloggingsløsning. Med en Feide-bruker benytter elever, studenter, forskere og undervisere ett og samme brukernavn og passord til å logge inn på alle tjenester som benytter Feide som innloggingsløsning. De slipper med andre ord å huske ulike brukernavn og passord for ulike tjenester.

Feide-brukere opprettes og endres av organisasjonen man tilhører og brukerinformasjon administreres og lagres lokalt hos organisasjonen. Hvis passord skal endres, gjøres ikke dette for hver tjeneste brukeren benytter, men én gang av organisasjonen.

I intervju med rådgiver i avdeling for IKT og dokumentasjonsforvaltning ble det opplyst at IFK har en formell passordpolicy i form av krav som ligger innbakt i Active Directory (AD). Det er ikke mulig å opprette passord i strid med disse kravene. Passordet må være på minst 9 tegn og inneholde tre av fire grupper:

- Små bokstaver
- Store bokstaver

[23] Feide er den nasjonale løsningen for sikker innlogging og datadeling i utdanning og forskning.
[24] Unit – Direktoratet for IKT og fellestjenester i høyere utdanning og forskning.

- Tall
- Tegn

Når det gjelder tidsbegrensning på passord så har de måttet utvide dette på grunn av Covid 19 og hjemmekontor-situasjonen. Ved bruk av hjemmekontor ble det vanskelig å opprette nye passord. Det er en avveining mellom vanskelige passord og hyppige bytter. Gjør man det for komplisert er det en risiko for at ansatte tar i bruk hjelpemidler som gule lapper etc. for å huske passordene sine. På tidspunktet for intervju var levealderen på passord ett år på grunn av hjemmekontor. Når situasjonen er tilbake til normalt vil de vurdere hvor ofte passordene bør byttes.

Brukernavn og passord lagres hos Feide organisasjonen, herunder IFKs Active Directory. Rådgiver i avdeling for IKT og dokumentasjonsforvaltning forklarer hvordan prosessen foregår med følgende eksempel:

1. Lærer logger inn i Visma InSchool med sin Feide-bruker (brukernavn og passord)
2. Visma InSchool sender en forespørsel til Feide
3. Feide videresender forespørsel til IFK
4. Forespørsel sees opp mot informasjonen som ligger i Feide katalogen og identifiseringen skjer mot lokal AD

Han forklarer at dette er en sikkerhetsmekanisme. Innbrudd i VIS vil ikke føre til at brukernavn og passord kommer på avveie, da disse ligger lagret i AD hos fylkeskommunen. Man må gjennom minst to brannmurer for å komme inn (Net Scaler) til AD.

På spørsmål om det er iverksatt to-faktorautentisering sier fylkeskommunen at det er besluttet iverksatt av Kompetanse og tannhelse, men av tekniske årsaker har implementering av dette blitt utsatt. I perioden revisjonen har vært utført har to-faktorautentisering ikke vært iverksatt. Innlandet fylkeskommune har fra skolestart høsten 2021 én Feide server, frem til da ble det benyttet én server for tidligere Oppland og én server for tidligere Hedmark.

ID-porten
ID-porten er en felles innloggingsløsning til offentlige tjenester på internett. VIGO og Conexus Oppfølgingsloggen bruker ID-porten for innlogging. ID-porten blir driftet av Digitaliseringsdirektoratet. For å logge seg inn via ID-porten må man ha en elektronisk ID som bekrefter identitet, det finnes seks alternativer for elektronisk ID:

- MinID
- BankID
- BankID på mobil
- Buypass
- Buypass på mobil
- Commfides

Felles for alternativene er at de alle er personlige elektroniske ID-er som gir tilgang til offentlige tjenester på et betydelig til høyeste sikkerhetsnivå.

4.2.3 SIKKERHETSOVERVÅKING

Når det gjelder sikkerhetsovervåkning for å avdekke sikkerhetshendelser relatert til tilgangskontrollen, er det ifølge personvernkoordinator i fylkeskommunen ingen aktiv sikkerhetsovervåking i form av alarmer ol. som skal følges opp. I Microsoft Office 365 er det logging av brukeraktivitet slik at ved en hendelse vil det i etterkant være mulig å bruke revisjonslogg til å kartlegge hva som har skjedd. Eventuell kontroll og overvåkning av tilgangsstyring til systemer med skyløsning skjer hos leverandør. Innlandet fylkeskommune har ingen egen sikkerhetsovervåking eller kontroll for å avdekke sikkerhetshendelser relatert til tilgangskontrollen.

Revisjonen har mottatt databehandleravtaler mellom fylkeskommunen som behandlingsansvarlig og databehandler i systemene Visma InSchool, Conexus Engage og VIGO. Ifølge avtalene har databehandler ansvar for jevnlig og på eget initiativ foreta revisjon av systemet som benyttes til behandling av personopplysninger. Behandlingsansvarlig kan revidere databehandleren inntil en gang i året. Databehandleren skal oppfylle alle krav til sikkerhetstiltak som stilles i personvernregelverket. Dette inkluderer å sette i verk tiltak som kreves i henhold til personvernforordningens artikkel 32 for å sørge for å oppnå et passende sikkerhetsnivå ut fra personvernrisikoen. Databehandleren skal blant annet loggføre og dokumentere alle forsøk på ikke-autorisert tilgang og andre brudd på personvern i datasystemene. Brudd på personvern skal uten ugrunnet opphold informeres om til behandlingsansvarlig.

Enhetsleder Digitale tjenester opplyser at databehandleravtalen med Conexus ble revidert og signert i april 2021 etter personvernavvik i 2020. Da ble det også på bestilling/initiativ av de berørte fylkeskommunene gjennomført en uavhengig sikkerhetstest av løsningen, samt en revisjon av leverandørens sikkerhetstiltak. Det ble utført av de berørte fylkeskommunene. Videre pågår det per november 2021 en revidering av databehandleravtaler med Vigo IKS.

Det er ifølge personvernkoordinator ikke etterspurt dokumentasjon fra sikkerhetsrevisjoner gjennomført av databehandler.

4.2.4 REVISJONENS VURDERINGER

Fylkeskommunen bør ha en overordnet retningslinje eller policy for tilgangsstyring

Fylkeskommunen bør ha en overordnet retningslinje eller policy for tilgangsstyring som en del av styringssystemet for informasjonssikkerhet. Denne bør som minimum inneholde rutiner for tildeling, endring, sletting og kontroll av tilganger, samt ansvarsfordeling innen tilgangskontrollen.

Fylkeskommunen har ikke overordnede retningslinjer eller policy for tilgangsstyring som en del av styringssystemet for informasjonssikkerhet og revisjonskriteriet er ikke oppfylt.

Fylkeskommunen har en etablert praksis for elementer av hva en overordnet retningslinje bør inneholde ved at de har formelle prosesser for opprettelse, endring og deaktivering av brukerkontoer i VISMA HRM, samt at alle brukertilganger lagres i et register (Active Directory). Dette er ikke nedfelt i en retningslinje eller skriftliggjort, og revisjonen vurderer at det er en svakhet at dette kan bli personavhengig. Fylkeskommunen mangler en tydelig ansvarsfordeling innen tilgangskontrollen, det foreligger ikke rutine for jevnlig gjennomgang av brukerrettigheter.

Fylkeskommunens retningslinjer og rutiner/policy for tilgangsstyring bør være basert på en overordnet informasjonsklassifisering som kategoriserer informasjon innen konfidensialitet, integritet og tilgjengelighet, og som styrer systemenes sikkerhetsnivå.

Fylkeskommunen har ingen overordnet retningslinje eller policy for tilgangsstyring, revisjonen har derfor ikke grunnlag for å vurdere om retningslinjen er basert på en overordnet informasjonsklassifisering.

Fylkeskommunen bør ha et system for brukeridentiteter og passord, all tildeling av rettigheter til tilgang bør registreres i et register.

Innlandet fylkeskommune har en formell passordpolicy med krav til passord som er innbakt i systemet (Active Directory), det er ikke mulig å opprette passord i strid med kravene. Revisjonen har ikke mottatt noe skriftlig dokumentasjon som omhandler fylkeskommunens passordpolicy.

Innlandet fylkeskommune benytter Active Directory (AD), Feide og ID-porten for innlogging til systemer som behandler elevdokumentasjon. I tillegg skal det være multifaktor pålogging til Microsoft Office 365. Feide har mulighet til to-faktor autentisering. Dette er besluttet satt i verk, men av tekniske årsaker har implementering av to-faktor autentisering blitt utsatt.

Revisjonen vurderer at fylkeskommunen i noen grad oppfyller revisjonskriteriet ved at de har etablerte passordregler og at tildeling av rettigheter registreres i standard AD-oppsett (Active Directory) med tilgangsgrupper og policyer. Samtidig er det en svakhet at det ikke er nedfelt noe skriftlig på dette området. Videre vurderer revisjonen at det er en stor svakhet at to-faktor autentisering ikke er aktivert for pålogging til Feide, som gir tilgang til et stort antall systemer.

Fylkeskommunen bør ha etablert sikkerhetsovervåking for å avdekke sikkerhetshendelser relatert til tilgangskontrollen.

Fylkeskommunen har ingen aktiv sikkerhetsovervåkning eller kontroll for å avdekke sikkerhetshendelser relatert til tilgangskontrollen. Eventuell kontroll og overvåkning av tilgangsstyring til systemer med skyløsning skjer hos leverandør. Fylkeskommunen har databehandleravtaler som regulerer leverandørens ansvar. Det har i noen grad vært gjennomført revisjoner av databehandleravtaler fra fylkeskommunens side, men det er ikke fulgt opp om databehandler har utført sikkerhetsrevisjoner iht. avtalen.

Revisjonen vurderer at revisjonskriteriet ikke er oppfylt. Selv om fylkeskommunen har databehandleravtaler så er det sårbart å overlate alt ansvaret for sikkerhetsovervåkning til leverandør av IKT-løsningene, uten at dette jevnlig blir fulgt opp.

4.3 RUTINER OG PRAKSIS FOR KONTROLL AV TILGANGSSTYRING I UTVALGTE IKT-SYSTEMER

I dette delkapittelet svarer vi på problemstilling 3:

> I hvilken grad er det etablert rutiner og praksis for kontroll av tilgangsstyringen i utvalgte IKT-systemer som behandler personopplysninger om elever i videregående opplæring?

I denne problemstillingen ser vi nærmere på fire utvalgte IKT-systemer og i hvilken grad det er etablert rutiner og praksis i fylkeskommunen og de enkelte videregående skolene for kontroll av tilgangsstyringen. Vi har utledet følgende revisjonskriterier som vi undersøker IKT-systemene og fylkeskommunens praksis opp mot:

1. Tilgangsstyringen i IKT-systemet skal være innrettet i henhold til risikovurdering av informasjonsverdiene i systemet.
2. Fylkeskommunen bør ha implementert en formell prosess for å registrere brukere som gis tilgangsrettigheter og for forvaltning av brukertilganger i IKT-systemet. Prosessen bør omfatte hele livssyklusen til en brukerkonto. Retningslinje for tilgangskontroll og prosess for administrasjon av kontoer, tilganger og rettigheter bør dokumenteres og være kjent i virksomheten.
3. Tilgang til IKT-systemer skal være basert på tjenstlig behov.
4. Fylkeskommunen skal ha oversikt over hvem som har tilgang til de utvalgte IKT-systemene og hvem som har gitt tilgang.
5. Fylkeskommunen skal ha et system for jevnlig kontroll og gjennomgang av om tildelte tilganger i IKT-systemet er korrekte.
6. Fylkeskommunen skal ha kontroll på service-/systemkontoer, utviklere og driftsbrukere og hvilke rettigheter disse kontoene har. Det bør ikke tildeles administratorrettigheter til sluttbrukere.
7. IKT-systemets bruker- og administratorkontoer som forvalter sensitive personopplysninger skal være beskyttet av sterk autentifisering.

Revisjonen har valgt å undersøke nærmere tilgangsstyringen i IKT-systemene Visma InSchool, Conexus Engage og Oppfølgingsloggen, og VIGO[25]. Vi vil i det følgende presentere funnene knyttet til det enkelte system for seg. Conexus Engage og Oppfølgingsloggen behandles sammen da disse systemene felles er en del av arbeidsprosessen med IKO-modellen i videregående skole. Informasjonen er basert på intervjuer ved seks utvalgte skoler, og i sentraladministrasjonen i fylkeskommunen.

4.3.1 VISMA INSCHOOL

4.3.1.1 Risikovurdering

Ifølge prosjektleder for innføringen av Visma InSchool (VIS) i Innlandet fylkeskommune gjør VISMA, som er leverandør av VIS, og innføringsprosjektet sentralt, fortløpende risikovurderinger når ny funksjonalitet i systemet iverksettes. Det er ikke fastlagt noen fremtidig plan for risikovurderinger i VIS når prosjektet går over til drift.[26]

Innlandet fylkeskommune gjennomførte vinteren 2020 en DPIA[27] for å vurdere personvernkonsekvenser i VIS. Der ble roller og tilgangsstyring pekt på som områder med stor risiko, spesielt for de som er administrativt ansatte, da disse i stor grad får sine tilganger tilpasset manuelt. Rollene som elev og lærer ble vurdert med lavere risiko når det gjelder tilgangsstyring, da disse rollene gis automatisk. Risikoer som ble avdekket i DPIA er fulgt opp med tiltak, ifølge prosjektleder for innføringen av VIS. Tiltakene knyttet til tilgangsstyring, var blant annet opplæring og oppfølging av de ansvarlige ute på skolene, samt jevnlig gjennomgang av tilgangslister av leder. I tillegg var behandlingsansvarliges vurdering at tilgangsstyring måtte følges spesielt tett opp i det videre arbeidet med VIS.

4.3.1.2 Rutine for tilgangsstyring i Visma InSchool

Innlandet fylkeskommune var i ferd med å ferdigstille en skriftlig rutine for tilgangsstyring i Visma InSchool da revisjonen hadde intervju med prosjektleder for innføring av VIS i Innlandet fylkeskommune, i april 2021. Rutinen *Roller og tilganger i Visma InSchool* ble ifølge prosjektleder presentert for skolene via Teams 22. april 2021. Revisjonen avventet på bakgrunn av dette intervju med skolene til siste halvdel av mai, for at de skulle få noe tid til å gjøre seg kjent med rutinen før intervjuene.

Rutinen har til hensikt at de ulike brukergruppene[28] som benytter Visma InSchool er gitt korrekte tilganger i systemet. Den beskriver blant annet ansvaret til ulike roller ved både fylkesadministrasjonen og den enkelte skole:

- *Tjenesteansvarlig for VIS* i Kompetanse og tannhelse er eier av dokumentet og er ansvarlig for at dette dokumentet er oppdatert.
- *Systemansvarlig VIS* har ansvar for å gjøre den praktiske jobben med å tildele korrekte roller og tilganger i VIS for ansatte i sentraladministrasjonen i IFK på bakgrunn av det den ansattes nærmeste leder har bestemt.

[25] VIGO med modulene VIGO Opplæring og VIGO skole
[26] Visma InSchool utrulleres til alle landets fylker i perioden 2019-2023.
[27] Data Protection Impact Assessment (DPIA) – en vurdering av personvernkonsekvenser som skal sikre at personvernet til de som er registrert i løsningen ivaretas, jf. personvernregelverket og GDPR artikkel 35.
[28] Visma InSchool brukes av skoleeiere, skoleledere, lærere, elever og foresatte.

- *Rektor* ved den enkelte skole er ansvarlig for at ansatte ved egen skole er gitt korrekte tilganger i VIS, og at tilgangene er begrenset til det man har tjenstlig behov for.

- *Skoleansvarlig for tilgangsstyring i VIS* - En til to dedikerte personer utpekt av skolens rektor har ansvar for å ajourholde roller og tilganger ved egen skole. Det er bare disse som skal ha tilgang i VIS til å endre øvrige ansattes tilganger.

- *Ansattes nærmeste leder* har ansvar for å vurdere hva slags tilganger medarbeidere trenger ut fra tjenstlige behov. For skoler vurderes dette i samarbeid med rektor og den som ajourholder roller og ansvar på egen skole. For sentraladministrasjonen vurderes dette i samarbeid med systemansvarlig VIS.

- *Den enkelte ansatte* har ansvar for å bruke systemet i henhold til eget tjenstlig behov og melde fra ved behov for endring av tilgang, både ved behov for økte og reduserte tilgangsrettigheter.

HRM-systemet[29] er master for alle personalopplysninger, dette innebærer at alle som skal bruke VIS som lærer eller annen ansatt ved skolen må være registrert i HRM-systemet for å få tilgang til VIS. VIS har organisert tilganger i et system bestående av roller og tilgangsgrupper. For et mer finkornet nivå kan man også knyttes til spesifikke persongrupper.

Roller og tilganger i VIS

Tilgangsstyringen skjer automatisk via systemet for de store brukergruppene av VIS; lærere, elever og foresatte. For ledelse, administrativt personell og rådgivere ute på skolene trengs det tilpassede tilganger for at de ansatte skal få løst sine oppgaver. Dette reguleres gjennom ulike roller og tilgangsgrupper i systemet som blir nærmere beskrevet nedenfor.

Det skilles mellom tre kategorier for tilganger i VIS:

- *Roller:* hovedgrupper som f.eks lærer-rolle (rollen er ikke finmasket nok dersom man har andre oppgaver enn på skolen enn å undervise).
- *Tilgangsgrupper:* Et sett med tilganger i tillegg til rollen man har.
- *Persongrupper:* Brukes spesielt for rådgivere der man får tilgang til personer utenfor sin klasse.

Alle brukere som legges inn i systemet får tildelt en av de forhåndsdefinerte **rollene**. Hver rolle har et gitt standard-sett av tilganger (rettigheter) i systemet, disse kan både omfatte lese- og skrivetilganger.

Revisjonen har mottatt et Excel-ark fra prosjektleder for VIS med oversikt over alle tilganger som er knyttet til de ulike rollene. **Hovedrollene** i systemet har følgende antall standard-sett av tilganger[30]:

- Skoleleder: 239 tilganger
- Admin: 49 tilganger
- Standardrolle: 12 tilganger
- Privatistadministrasjon: 82 tilganger
- Lærer: 87 tilganger

[29] Visma HRM

[30] Oversikten er datert 18. mars 2021

Betegnelsen «Administrator» brukes som regel for den rollen som har alle rettigheter og tilganger i et system. I Visma InSchool er det rollen «Skoleleder» som har administrator-rettigheter. Rollen «Admin» er en rolle som skal være tilpasset ansatte som jobber med administrasjon ute på skolene.

I tillegg finnes det følgende roller som systemet tildeler automatisk utfra opplysninger som registreres om vedkommende i VIS:

- Elev – alle elever gis automatisk rollen elev
- Kontakt (foresatt) – alle som hentes inn eller manuelt registreres som kontakt/foresatt får rollen kontakt.
- Sensor
- Vakt

Dersom man har behov for tilganger utover det som ligger i rollen knyttes man til tilgangsgrupper. Alle tilgangsgrupper må opprettes av skoleeier. Tilgangsgruppene fungerer likt uavhengig av hvilken standardrolle man har i bunn. Enkelt-tilganger kan ikke tildeles direkte til en ansatt i VIS, man må legges inn i tilgangsgrupper for å få nødvendig tilgang i systemet.

Enhetsleder for Digitale tjenester forteller at Visma og fylkene har en egen referansegruppe som jobber kontinuerlig med å definere hvilke tilganger som skal ligge i den enkelte rolle, og hvilke tilganger som skal ligge i tilgangsgrupper. Dette arbeidet påvirker antall tilganger per rolle. Siden systemet er under utvikling opprettes også nye tilganger, og da vurderer referansegruppen om nye tilganger skal ligge til en rolle eller i en tilgangsgruppe. Antall standard-sett av tilganger og roller som det vises til i dokumentet fra 18. mars 2021 vil derfor kontinuerlig være i endring.

Opprettelse og vedlikehold av brukertilganger på skolene

To av seks skoleansvarlige for VIS som vi intervjuet var kjent med rutinen for tilgangsstyring når intervjuene ble gjennomført i siste halvdel av mai 2021.

Ifølge de skoleansvarlige for VIS er det mellom en til tre personer ved hver skole som har ansvar for å styre tilganger i VIS. Samtlige ved de seks skolene opplevde at de har god oversikt over nytilsettinger, endringer av arbeidsforhold og avslutning av arbeidsforhold som påvirket tilganger i VIS.

<u>Opprettelse av brukertilganger på skolene</u>
De skoleansvarlige i VIS sier i intervjuene at alle ansatte ved skolen automatisk får en brukertilgang i VIS når de er registrert som lønnsmottaker i Innlandet fylkeskommunes HRM-system. Alle ansatte som blir overført fra HRM-systemet til VIS har rollen *lærer*. Dersom vedkommende skal ha en annen rolle må skoleansvarlig for VIS endre dette manuelt. Dette gjelder alle andre enn det pedagogiske personalet ved skolen, slik som ansatte i administrasjon og ledelse, rådgivere, renholdspersonell, vaktmester, kantinepersonell og eksamensvakter.

En ansatt med rollen lærer vi kun ha tilgang til elever som han eller hun er knyttet til i timeplanen. For ansatte med stillingen lærer så gjør ikke skoleansvarlig noe mer tilpasninger av tilgangen, lærere får automatisk riktige

tilganger basert på fag og klasser de blir koblet opp til i timeplanen. Unntaket er for kontaktlærere der skoleansvarlig manuelt legger til tilgang.

Vedlikehold av brukertilganger

Dersom det oppstår endringer i et arbeidsforhold som påvirker hvilke tilganger vedkommende skal ha i VIS må endringen gjøres manuelt av skoleansvarlig i VIS. Det var ulikt hvor mye erfaring de skoleansvarlige i VIS hadde med å gjøre endringer i brukertilganger. Ved noen skoler hadde det ikke vært endringer i arbeidsforhold som påvirket tilganger i VIS. Generelt var endringer av brukertilganger noe de skoleansvarlige opplevde at de ikke kunne godt nok enda.

Ifølge rutinen[31] skal det sendes melding til skoleansvarlig dersom noen slutter eller endrer rolle. Det var ikke iverksatt noe system eller rutine for å fange opp endringer i ansettelsesforhold ved de seks skolene revisjonen har gjennomført intervjuer. De skoleansvarlige (for VIS) opplevde det som litt tilfeldig om de mottar endringsmeldinger eller ikke. Samtidig mente de fleste skoleansvarlige at de hadde god oversikt over hva som rørte seg på skolen, og at de dermed fikk med seg om det skjedde endringer som kunne påvirke tilgang i VIS. De opplevde også at de fikk beskjed dersom noen hadde for få tilganger til å gjøre jobben sin.

Dersom en lærer bytter klasse eller fag gjennom året så vil tilgangen endres automatisk basert på informasjon i timeplanen i VIS. Endring i tilgang skjer automatisk til den klassen vedkommende er knyttet til i timeplan. Unntaket er for kontaktlærere da kontaktlærertilgang må legges til manuelt og vedlikeholdes manuelt.

Avslutning av brukerkonto i VIS

Det var noe usikkerhet blant de skoleansvarlige om brukerkonto i VIS ble avsluttet automatisk som følge av at den ansatte ble satt med sluttdato i HRM-systemet.

En av de intervjuede beskrev at «*Når det sendes personalmelding til skoleeier så deaktiverer skoleeier brukerkonto fra dagen etter at arbeidsforholdet opphørte. Man trenger ikke å gå inn i systemet for å avslutte tilganger».* Skoleansvarlig ved en annen skole forklarte at *«Det er automatikk i at ansatte kommer inn, men ikke ut, ansatte må derfor manuelt deaktiveres i VIS».* Ved en tredje skole beskrev skoleansvarlig at *«Avslutning av brukerkontoer skal i utgangspunktet skje automatisk, men det er ofte man må ligge litt lenger i HR-systemet pga. f.eks ferie til gode».*

Ifølge enhetsleder for Digitale tjenester i fylkeskommunen så får ansatt en sluttdato i HR-systemet når vedkommende slutter. Når sluttdato er passert, så blir selve brukeren inaktiv, og den ansatte får ikke lenger logget seg inn i VIS. En inaktiv ansatt som forsøker å logge seg inn i VIS får melding om at han/hun ikke er tilknyttet skolen.

4.3.1.3 Tjenstlig behov for tilganger

Ifølge rutine for tilgangsstyring i VIS er rektor ved den enkelte skole ansvarlig for at ansatte ved egen skole er gitt korrekte tilganger i VIS, og at tilgangene er begrenset til det man har tjenstlig behov for. Det er videre beskrevet i rutinen at enkelte ansatte i sentraladministrasjonen i Innlandet fylkeskommune innen

[31] Rutine for tilgangsstyring i VIS

Dokumentasjonsforvaltning, HR og Kompetanse og tannhelse har behov for tilgang til VIS for å kunne løse sine arbeidsoppgaver. Disse må gis skoleeier-rolle.

I praksis er det de skoleansvarlige i VIS som sørger for at tilganger i systemet er korrekte. De var bevisste på at tilganger i VIS skal være i henhold til tjenstlig behov. Flere av de skoleansvarlige som revisjonen intervjuet opplevde at tilganger ofte ble gitt reaktivt, ved at den ansatte ga beskjed om at han/hun manglet tilgang. Skoleansvarlig ved en av skolene beskrev, «*Forsøker hele tiden å ha GDPR i bakhodet, kan iblant gjøre det vanskelig ved at de ansatte opplever at de tidvis har for lite tilganger. Prøver alltid å tenke need to have, not nice to have".*

De skoleansvarlige opplevde at de ulike tilgangsgruppene hadde blitt finmasket, men at det er vanskelig å få de så finmasket at man unngår at noen har tilganger de strengt tatt ikke skulle hatt. De hadde opplevd at det tok tid å finne ut hvilke tilganger det er behov for i de ulike rollene. Ved oppstart høsten 2020 måtte mange ansatte ved skolene ha skoleleder-rolle for å kunne gjøre jobben sin. Dette gjaldt spesielt administrativt ansatte som avdelingsledere, merkantile og rådgivere. Grunnen til det var at rollen som «Admin» ikke hadde tilstrekkelige tilganger til at de kunne gjøre alle oppgaver som lå til stillingen sin. Dette opplevde skoleansvarlige som utfordrende da dette i praksis ga de alle tilganger i systemet.

En skoleansvarlig beskrev at «*Ved oppstart av VIS var ikke roller og ansvar helt klart, så alle i administrasjonen og rådgivere hadde skoleleder-rolle. Dette opplevde de som ugreit. Dette er strammet inn og det er gjort en god jobb både fra lokalt innføringsteam og VIS».* En annen skoleansvarlig forklarte at skolen hadde vært i dialog med fylket når det gjaldt tilganger for avdelingsledere. Avdelingslederne måtte en periode ha skoleleder-rolle for å utføre arbeidsoppgavene sine. Tilsvarende måtte ansatte som arbeider med eksamensadministrasjon ha skolelederrolle for å gjøre oppgavene sine. Disse skal på sikt ha admin-rolle og knyttes til riktig tilgangsgruppe.

<u>Revisjonens kontroll av tilganger</u>

Revisjonen gjennomførte en kontroll av om tilganger i systemet var basert på tjenstlig behov ved de utvalgte skolene. For å undersøke dette sjekket vi, i samarbeid med skoleansvarlig i VIS, om brukerkontoen til ansatte som hadde sluttet ved skolen skoleåret 2020/2021 var deaktivert og hvor mange ansatte ved skolen som hadde utvidede privilegier i systemet. Vi så spesielt på rollen *skoleleder* da denne rollen har flest tilganger i systemet.

Det var ingen av skolene revisjonen hadde plukket ut som hadde iverksatt en rutine for å deaktivere tilganger når ansatte sluttet. Det var et ulikt antall ansatte som hadde sluttet i løpet av skoleåret 2020/2021, fra ingen ansatte til 37 ansatte. Et stort flertall av brukerkontoer til ansatte som hadde sluttet i løpet av skoleåret var fortsatt aktive da skoleansvarlig og revisor gikk gjennom tilgangene. Ved enkelte av skolene hadde tilganger blitt deaktivert, dette gjaldt spesielt for personer som jobbet administrativt i skolen.

I gjennomgangen av brukerkontoer i VIS gikk revisjonen og skoleansvarlig gjennom alle ansatte med rollen skoleleder. Ved fire av skolene anså skoleansvarlig at antallet med skoleleder-rolle var riktig og at alle med denne rollen hadde behov for utvidet tilgang. Dette omfattet i hovedsak rektor, avdelingsledere og skoleansvarlig i VIS. Ved to av skolene var det ansatte med skoleleder-rolle uten tjenstlig behov. Videre var det flere ansatte med skoleleder-rolle som kun hadde denne rollen midlertidig fordi de hadde oppgaver som krevde denne tilgangen i forbindelse med eksamen, karakteroppgjør og inntak.

I gjennomgangen av skoleleder-rollen så man at det i tillegg til ansatte ved skolene, var ansatte fra skoleeier (IFK) som hadde skoleleder-rolle ved skolene. Antallet varierte mellom skolene, fra fem til ni. Ifølge medarbeider som har spesielt ansvar for tilganger i innføringsprosjektet, er det fire ansatte fra IFK som skal ha skoleleder-rolle ved alle VGS for å gjøre support. I forkant av nytt skoleår er det i tillegg en fra Inntakskontoret, samt en som har support på timeplanlegging som skal ha tilgang.

Ved én skole hadde de opplevd at elever kom inn i systemet med rollen lærer. Dette kunne skje fordi de eksempelvis hadde sendt reiseregning som var behandlet i Visma HRM. Dersom man mottar lønn eller andre ytelser fra skolen kommer man automatisk inn i VIS med lærer-rolle. Skoleansvarlig ved denne skolen går derfor gjennom listen over ansatte med tilgang den 12. hver måned, for å se om det har kommet inn elever i systemet som ikke skal være der. Elevene som får lærer-rolle i VIS vil ikke kunne se opplysninger om andre elever da de ikke er knyttet til en undervisningsgruppe i timeplanen.

Flere revisjonen intervjuet ute på skolene opplever at tilgangsstyringen i VIS er krevende. Et av intervjuobjektene beskriver det slik; «*Oppleves som veldig innviklet det med roller og tilganger i VIS. Finnes flere forskjellige roller med fast bestemte tilganger, kan i tillegg gi ulike gruppe-tilganger til rollene. Ikke alle tilgangene har fungert tilfredsstillende. Må ha tunga rett i munnen».*

Visma in School benytter Feide for pålogging. Det er ikke satt i verk to-faktor autentisering i Feide og det er ikke krav om egne passord for administratorkontoer. I systemer som bruker Feide for pålogging opplyses det om at det ikke er mulig å ha to ansatt-brukere, som betyr at det ikke skilles mellom vanlig brukerkonto og administratorkontoer i VIS. En ansatt som bruker VIS både som vanlig bruker, men også har administrator-oppgaver eller systemansvar i VIS, har derfor en brukerkonto med utvidede rettigheter.

Revisjonen har fått opplysninger fra enhetsleder for Digitale tjenester i fylkeskommunen at det i september 2021 ble utviklet ny funksjonalitet for å kunne gi en ansatt en tilleggsrolle i VIS. Denne funksjonen fungerer slik at de ansatte kan bytte rolle etter at de har logget inn i løsningen. Det betyr at begge rollene fortsatt har samme innlogging via Feide. Fylkeskommunen har vurdert at funksjonen ikke gir bedre sikkerhet, men noe ryddigere funksjonalitet med tanke på menyer/arbeidsoppgaver. Funksjonen er derfor i svært liten grad tatt i bruk på skolene.

4.3.1.4 System for jevnlig kontroll og gjennomgang av tildelte tilganger i Visma inSchool

Ansatte med rollen skoleleder i VIS kan ta ut rapporter over alle ansatte som har tilgang i systemet, herunder oversikt pr. ansatt, oversikt basert på rolle og oversikt basert på tilgangsgruppe. Alle revisjonen intervjuet var kjent med denne funksjonen. Det var ikke kjent om man kunne se hvem som har gitt tilgangen eller når tilgangen ble gitt. Ifølge lokalt innføringsteam så er det ikke mulig å ta ut logg for dette lokalt, men man kan få det på forespørsel fra Visma sentralt.

Rutine for tilgangsstyring i VIS beskriver kontroll og gjennomgang av tildelte tilganger ute på skolene. Rutinen sier at skoleeier har ansvar for gjennomgang/kvalitetssikring av at tildelte roller og tilganger på skoleeiernivå er korrekte og i tråd med rutinen. Gjennomgang og kontroll av tilganger må gjøres jevnlig, og minimum en gang pr skoleår.

På tidspunktet revisjonen gjennomførte intervjuene med skoleansvarlige var det ingen av de seks som hadde iverksatt en rutine for å kontrollere om tilganger var korrekte. De fleste skoleansvarlige opplevde likevel at de hadde god oversikt over tilgangene i systemet. De mente også at oppstart av nytt skoleår ville være et naturlig tidspunkt for gjennomgang av tilganger. Ved overgang til nytt skoleår beholder alle ansatte som ikke er koblet opp til klasser/elever i timeplanen tilgangen i VIS. Lærere mister automatisk tilgang til elever de ikke lenger underviser ved skoleslutt. På samme måte får de tilgang til nye elever ved at de blir koblet opp til undervisningsgrupper i timeplanen i VIS. Samtidig var det noen som pekte på viktigheten av at det innarbeides rutine for å rapportere om endringer ved endringer i ansettelsesforhold som påvirker tilganger gjennom skoleåret.

Revisjonen spurte om fylkeskommunen har kontroll på service-/systemkontoer, utviklere og driftsbrukere i VIS, og hvilke rettigheter disse kontoene har. Ifølge prosjektleder for innføring av VIS er det Visma sentralt som drifter systemet og IFK har derfor ikke ansvaret for service-/systemkontoer, utviklere og driftsbrukere.

4.3.2 CONEXUS ENGAGE OG OPPFØLGINGSLOGGEN

4.3.2.1 Risikovurdering

Ifølge systemeier for Conexus Engage (Engage) i IFK foreligger det ingen plan for når og hvor ofte fylkeskommunen skal gjennomføre risikovurderinger av Engage og Oppfølgingsloggen. I forbindelse med sikkerhetsbruddet i Engage i 2020 ble det gjort en risikovurdering av alle fylkeskommunene som er med i IKO-prosjektet. Der ble det understreket hvor viktig registreringen i Visma InSchool er og at dette blir gjort riktig. De gjorde også en verdivurdering av all informasjon i systemet, der tilgang og rollebeskrivelser ble grundig diskutert. Det ble ifølge systemeier gjort noen tiltak i etterkant, blant annet når det gjaldt registrering i VIS og hvor mange som hadde behov for å importeres til Engage. På bakgrunn av dette ble dataimporten endret til å kun gjelde pedagogisk ansatte. Tidligere ble alle ansatte ved skolen importert til Engage.

Revisjonen har mottatt dokumentene; *Konsekvensvurdering for personvern i Engage*[32] og *Verdivurdering Engage* fra fylkeskommunen.

I *Konsekvensvurdering for personvern i Engage* er det vurdert som risiko at personopplysninger kan komme på avveie utenfor organisasjonen eller at eksterne personer får tilgang til opplysninger de ikke skal ha tilgang til, f.eks. pga. hacking. I beskrivelsen av punktet står det: «*det er gjort mange tiltak for å sikre opplysningene. Det er to-faktor pålogging (Feide). Sårbarheter i utvikling og drift er ikke tilstrekkelig fulgt opp»* Fylkeskommunen skriver i begrunnelsen: «*hendelsen i mai 2020 viste at dette kunne skje. Sannsynligheten er lavere nå, da leverandør vil ha økt fokus på sikkerhet. Fylkeskommunen vil også i dag ha mer fokus på oppfølging av leverandøren».* Det fremgår ikke tiltak eller ansvarlig for dette punktet.

Systemansvarlig i Engage forteller at de etter sikkerhetsbruddet har hatt hyppigere kontakt med leverandør av systemet, i møtene med leverandør tar de opp eventuelle feil, mangler eller andre problemer. I *verdivurdering Engage* fremgår det at personopplysninger i Engage har blitt vurdert to ganger, henholdsvis i 2019 og 2020.

[32] Av 13.10.2020

Enhetsleder for Digitale tjenester i fylkeskommunen påpeker at selv om ansatte blir importert til Engage fra Visma InSchool får de ikke automatisk tilgang til elevinformasjon. Tilgang til elevinformasjon forutsetter relasjon mellom den ansatte og eleven i Visma InSchool, eller manuell tildeling i Engage.

4.3.2.2 Rutine for tilgangsstyring i Engage

Det er leder i avdeling for Kompetanse og tannhelse som formelt er systemeier for IKT-systemet og har ansvaret for tilgangene i Engage, men det er en ansatt ved avdeling for Kompetanse og tannhelse som i praksis utfører ansvaret i systemet. Systemeier i IFK gir administratortilganger til hver skole, henholdsvis til rektor eller annen leder ved skolen, heretter kalt skoleadministrator.

Det er 4 skoleeieradministratorer og 131 skoleadministratorer i systemet. De 131 skoleadministratorene fordeler seg på 28 ulike enheter. Noen av disse skoleadministratorene har denne rollen på flere enheter (for eksempel Lillehammer nord og Lillehammer sør). Antallet skoleadministratorer endrer seg jevnlig med oppsigelser og endringer i ansettelsesforhold.

Ifølge systemeier for Engage foreligger det ikke noen skriftlig rutine for hvordan tilganger skal tildeles, endres eller deaktiveres i Engage. Tilganger i systemet går gjennom det skoleadministrative programmet Visma InSchool (VIS) og alle pedagogisk ansatte i skolen får en rolle i Engage basert på hvilke rettigheter de har i VIS. Disse rettighetene overføres til Engage. En lærer skal derfor bare se sine egne elever. Rektorene har ansvaret for at de legger riktig informasjon i VIS.

I intervjuene med skoleadministratorene går det fram at det er noe ulik forståelse for hva som er skoleadministrators ansvarsområde når det gjelder tilgangsstyring i Engage. Noen av skoleadministratorene oppfatter at all tilgangsstyring i Engage går gjennom VIS og de tildeler derfor ikke selv tilganger eller roller i Engage. Andre mener at alle tilganger må legges inn manuelt av skoleadministrator; «*det er ingen automatikk i systemet, snakker ikke med VIS, så alle tilganger må legges inn manuelt».*

Roller og tilganger i Engage

Tabellen nedenfor illustrerer de ulike rollene/funksjonene i Engage. Skoleadministrator kan endre tilgang til brukere, herunder legge til og slette tilganger, men ikke endre systemet.

	Skolenivå				**Skoleeiernivå**	
Funksjon	**Resultat-registrering**	**Resultat-registrering «Fag og fravær»**	**Admin.**	**Rapporter og status**	**Rapporter og status**	**Admin.**
Faglærer	x					
Kontaktlærer	x	x				
Avdelingsleder	x	x				
IKO-ansvarlige, rådgivere (elevtjeneste)	x	x		x		
Skoleadministrator	x	x	x	x		

	Skolenivå				Skoleeiernivå	
Skoleledere (rektor, ledergruppe etc.)	x	x	x	x		
Administrator (registeransvarlig)						x
Skoleeier					x	x
IKO-analytiker	x				x	

Det er i tillegg mulig å velge om tilgangen skal gjelde alle elever eller begrenset (kun sin egen gruppe). IKO-ansvarlig, skoleleder og skoleeier vil i utgangspunktet ikke ha noen tilganger i Engage, forutsatt at personen ikke også er faglærer eller kontaktlærer. Tilgang for disse brukerne må settes manuelt av skoleadministrator eller skoleeieradministrator. Faglærer vil kun ha tilgang til å registrere midtveisvurderinger for eget fag og tilgang til å sende bekymringsmelding til Oppfølgingsloggen. En kontaktlærer vil ha tilgang til å sende bekymringsmelding, se fag og fravær for egen basisgruppe, samt til identifiserings- og kartleggingsverktøy for egen basisgruppe.

I tillegg til ansatte ved skolen har også fylkeskommunalt ansatte PP-rådgivere og helsesykepleiere tilgang til Engage. De bruker Feide for pålogging og skoleadministrator gir tilgang.

I Oppfølgingsloggen styres ikke roller og rettigheter av tilganger nevnt over. I Oppfølgingsloggen er tilganger basert på rollene *oppfølgingsansvarlig, aktør, skoleleder og skoleeier*. Manuelle tilganger til aktører i hver enkelt sak gis av oppfølgingsansvarlig/skoleadministrator. Det er én oppfølgingsansvarlig på hver skole. Dette betyr at fag- og kontaktlærer ikke har tilgang til Oppfølgingsloggen med mindre de blir tildelt tilgang i den enkelte oppfølgingssak.

<u>Opprettelse og vedlikehold av brukertilganger på skolene</u>

Ifølge systemeier er Engage integrert med det skoleadministrative systemet (VIS) som har Visma HRM som master for ansattinformasjon. Brukerkonto blir opprettet i VIS og overført til Engage. Det er ingen brukerkontoer som blir opprettet manuelt i Engage. Det er administrator ved den enkelte skole som har ansvaret for å tildele riktig tilgang til de ansatte. Alle ansatte ved skolen ligger automatisk inne i Engage og korrekt registrering i det skoleadministrative systemet (VIS) skal gi riktige tilganger til elevopplysninger i Engage. Det kan bli gitt manuelle tilganger til systemet av administratorer både på fylkesnivå og skolenivå, men det er i stor grad VIS som styrer tilgangene. Unntaket er om noen bytter arbeidsplass, eller i tilfeller der lærere ikke er korrekt lagt inn i VIS, da gis det manuell tilgang til riktig elevgruppe.

Frem til oppstart av nytt skoleår er brukere registrert, men har ingen tilganger til undervisningsgrupper. Skoleadministrator må derfor inn i systemet ved skolestart for å gi tilganger basert på fag og timefordeling hos den enkelte ansatte. Dette gjelder i hovedsak IKO-team.

Det foreligger ingen rutine eller formell prosess på skolene revisjonen har undersøkt for å gi skoleadministrator beskjed om endringer i ansattforhold som kan påvirke endringer i tilganger i Engage. Skoleadministratorene mente allikevel at de hadde god oversikt over endringer i ansattforhold ved at de organisatorisk var knyttet til ledergruppen ved skolen, eller at de ellers hadde god oversikt over personalet ved skolen. Enkelte av skoleadministratorene oppfatter at endringer skjer automatisk; «d*et er ingen rutine for det da det skjer så sjelden. Ellers så skjer dette automatisk også ved lærerbytte da tilgangen er knyttet opp til timeplan».*

Tilganger til undervisningsgrupper nullstilles hvert år og tilganger må gis på nytt. Brukerkontoen vil fortsatt være synlig i systemet, men uten tilganger til undervisningsgrupper. Ved avslutning av arbeidsforhold vil vedkommende bli avsluttet i Visma HRM, og deretter blir de avsluttet i VIS og videre i Engage.

Oppfølgingsloggen er bygd opp slik at det er tidsbegrensning på tilgangen knyttet til den aktuelle bekymringsmeldingen. Det gis kun tilganger til enkeltsaker og tilgangen følger saken til den er avsluttet. Systemet gir påminnelser ved at det blinker rødt slik at oppfølgingsansvarlig ved skolen skal bli påminnet om å avslutte tilgangen. Tilgang til aktører i Oppfølgingsloggen gis i IKO-møter (Identifisering, kartlegging, oppfølging) hver uke. Dette baseres på bekymringsmeldingene og hvem som skal følge opp tiltak i bekymringsmeldinger. Aktør er de som skal jobbe med den eleven det er sendt bekymringsmelding om (f.eks. lærer, rådgiver, skolehelsetjenesten). Det er oppfølgingsansvarlig som gir og avslutter tilganger i de ulike enkeltsakene.

4.3.2.3 Tjenstlig behov for tilganger

Ifølge dokumentet *«Tidlig innsats når det gjelder»* som er mottatt fra Innlandet fylkeskommune så skal alle fag- og kontaktlærere ha tilgang til Engage. Disse tilgangene skal følge tilganger i VIS. En lærer skal derfor kun ha tilgang til de klassene han/hun er lærer for.

Skoleadministratorene fortalte at de er avhengige av at tilgangene gitt i VIS er riktige, og at de opplever at disse stort sett er riktige. Dersom det ikke ligger opplysninger i VIS om hvilke klasser ansatte er knyttet til, eller om det ellers er mangelfullt registrert så får vedkommende «default» tilgang. Det vil si at man kommer inn, men man har ikke tilgang til å se noe. Det kan ifølge skoleadministratorene skje at man får tilgang til mer enn man har tjenstlig behov for, dersom man for eksempel endrer klasse underveis i skoleåret og det ikke blir oppdatert i VIS.

Det ble påpekt at alle ansatte ved skolen sto oppført som brukere i Engage, selv om de ikke var pedagogisk ansatte. Enkelte av skoleadministratorene nevnte at det også kunne dukke opp elever i oversikten over brukere i Engage. Disse elevene kommer inn i Visma HRM gjennom å ha sendt reiseregning og videre overføres til VIS og Engage. Elevene som kommer inn i Engage ved at de har sendt reiseregning får kun en brukerkonto, men ingen tilgang til elever. En systemansvarlig uttalte at det er «*synd at alle ansatte ved skolen inkludert renholdere, vaktmester, assistenter og elever som har sendt reiseregning er en del av ansattlisten i Engage».*

Engage benytter Feide for pålogging og påloggingen er eksponert på nett. Administratorkontoer er knyttet opp til vanlig brukerkonto, men med utvidet tilgang. Det er ikke satt i verk to-faktor autentifisering i Feide og det er ikke krav om egne passord for administratorkontoer. I systemer som bruker Feide for pålogging opplyses det om at det ikke er mulig å ha to ansatt-brukere, dette betyr at det ikke skilles mellom bruker og administratorkontoer i VIS.

For å sende bekymringsmelding fra Engage til Oppfølgingsloggen er det to faktor-autentifisering ved at man bruker ID-porten for innlogging.

<u>Revisjonens kontroll</u>
Revisjonen gjennomførte sammen med skoleansvarlig i Engage kontroll av om tilganger i systemet var basert på tjenstlig behov. Vi undersøkte om brukerkontoen til ansatte som hadde sluttet ved skolen skoleåret 2020/2021 var deaktivert, og om tilgang i Engage var oppdatert ved endringer i arbeidsforhold. Videre så vi på et tilfeldig utvalg av ansatte for å se om tilganger i Engage stemte overens med tilgangene i VIS.

I hovedsak var alle som hadde sluttet deaktivert eller fjernet fra listen over ansatte på de utvalgte skolene. Det var noen få som fortsatt lå inne i systemet, fordi de tidvis arbeidet ved skolen som vikarer/eksamensvakt. Disse hadde ikke tilgang til å se elever. Det var noe ulik praksis for hvordan skolene behandlet tilganger dersom ansatte var i permisjon. Noen hadde satt tilgangen til «ingen», som vil si at dersom den ansatte logger seg inn vil han/hun ikke ha tilgang til elever. Andre endret ikke tilganger når ansatte hadde permisjon.

Det var et lite antall ansatte ved skolene som hadde endret rollene sine i løpet av skoleåret, men disse hadde riktig tilgang sammenlignet med tilgangen i VIS.

I gjennomgangen av tilfeldige brukerkontoer fant vi at det i stor grad stemte overens med det som var registrert i VIS. Unntaket var at det ved enkelte skoler forelå færre tilganger i Engage, enn i VIS. Dette gjaldt spesielt skolene som mente at tilgangene ble styrt automatisk. Ved et par tilfeller hadde lærere tilgang til flere klasser enn de lå inne med i timeplanene i VIS.

4.3.2.4 System for jevnlig kontroll og gjennomgang av tildelte tilganger i Engage

Ansatte med administratorrettigheter i Engage kan se hvilke tilganger alle har i systemet, og skoleadministratorene hadde kunnskap om hvordan se hvilke rettigheter den enkelte har i systemet. Skoleadministratorene kjenner ikke til at det finnes en oversikt over når tilgangen ble gitt og hvem som har gitt tilgang. Siden tilgangene nullstilles ved overgang til nytt skoleår vet de at tilgangen ikke er mer enn ett år gammel.

Ifølge systemeier i Engage kan fylkeskommunen be leverandør av systemet om rapport over når og av hvem tilgang ble gitt. Dette ble gjort ved sikkerhetsbruddet i Engage. Systemeier har oversikt over hvem han har gitt administratortilganger til. Han har som rutine at han går inn i systemet for å sjekke at tilganger er avsluttet om en rektor slutter eller bytter skole. Dette er ikke skriftliggjort, men en etablert praksis.

Det foreligger ingen egen rutine for å kontrollere om tilganger i Engage er korrekte. Fordi tilgangene i Engage er basert på tilganger den enkelte ansatte har i VIS, er det ifølge systemeier rutinen i det skoleadministrative systemet VIS som styrer kontrollen av tilganger også i Engage.

De utvalgte skolene hadde ulik praksis for gjennomgang av tilganger i Engage. En skoleadministrator sa at vedkommende har «*tenkt at Engage snakker sammen med VIS, så har ikke hatt kontroll av tilganger. Stoler på at masterdata er riktig».* Enkelte går gjennom tilganger en gang i året i forbindelse med at tilgangene har blitt nullstilt. Andre gjennomfører hyppigere kontroll av tilganger og en skoleadministrator «*har kontroll av tilganger minst tre ganger pr. år, i forbindelse med oppstart og midtveisvurdering 1 og 2. Dersom det er endringer i et ansattforhold som påvirker tilganger pleier jeg å se over tilgangene».*

Revisjonen spurte om fylkeskommunen har kontroll på service-/systemkontoer, utviklere og driftsbrukere i Engage, og hvilke rettigheter disse kontoene har. Systemeier forteller at de forholder seg til to personer hos leverandøren av systemet som brukes til support og hjelp. IT-avdelingen i fylkeskommunen har ingen ansvar for drift og vedlikehold av systemet og har ingen tilganger i Engage. Det er leverandøren av systemet (Conexus) som har ansvaret for drift og vedlikehold.

4.3.3 VIGO

VIGO består av flere moduler som i en eller annen form håndterer personer i videregående opplæring. Revisjonen har valgt å se nærmere på modulene VIGO Opplæring og VIGO Skole, da det er disse modulene som i hovedsak blir brukt av fylkeskommunen og skolene.

VIGO Opplæring brukes av inntakskontoret i IFK i forbindelse med inntak til VGS. VIGO Opplæring styrer også informasjonen på vilbli.no, som viser hvilke skoler og linjer elevene kan søke på.

Både grunnskoler og VGS har tilgang til VIGO Skole, men de har kun lesetilgang. Det er systemansvarlige i VIGO Opplæring i IFK som styrer tilgangen til systemansvarlige ute på skolene. VIGO Skole brukes av skolene som et oppslagsverk for å se hvor mange søkere de har til nytt skoleår, og er et speilbilde av opplysninger som ligger i VIGO Opplæring. Skolene bruker i hovedsak VIGO Skole ved inntak vår/høst for å hente inntakslister og kontakte nye elever som skal starte på skolen. Rådgivere i VGS bruker systemet til å følge opp at elever ved skolen har søkt seg til neste trinn. Avdelingsleder og rektor følger med på søkerstatistikk. Hensikten er at skolene skal kunne se søkeprosessen i forkant av skolestart.

4.3.3.1 Risikovurdering

Systemeier og systemansvarlige i VIGO Opplæring sier at de ikke kjenner til at det foreligger en plan for å gjennomføre risikovurderinger i systemet, men de mener at det har blitt gjennomført risikovurderinger i noen moduler av VIGO sentralt. Innlandet fylkeskommune har gjennomført en vurdering av all informasjon i systemene for å kartlegge omfang av personopplysninger, men ikke gjennomført en risikovurdering i VIGO.

4.3.3.2 Rutine for tilgangsstyring i VIGO

Revisjonen har mottatt en intern beskrivelse av hvordan man går frem for å legge til en ny bruker i VIGO Opplæring. Beskrivelsen sier ikke noe om tilganger i systemet.

Det er to ansatte i fylkeskommunen som har rollen som systemansvarlig i VIGO Opplæring, og det er disse som styrer tilgangene i systemet. Ifølge disse opprettes en ny bruker ved at systemansvarlig får melding fra den nyansattes leder om at det skal opprettes en ny brukerkonto. Tilganger i systemet gis ut fra personens arbeidsoppgaver. Det kan tildeles lesetilgang til skolene ved behov. Det er spesielt voksenopplæringen som har behov for lesetilgang, da de bruker opplysningene som ligger i VIGO Opplæring som oppslagstavle.

I VIGO Skole er det ikke etablert en skriftlig rutine eller formell prosess for tilgangsstyring, men skoleadministratorene som revisjonen har snakket med opplevde at det var forholdsvis oversiktlig å styre tilganger i VIGO Skole. En skoleadministrator beskrev det på denne måten; «*lite styringsmuligheter av tilganger i systemet. Gir kun skolebruker-tilgang. Store deler av året brukes ikke systemet og opplysninger og tilganger er slettet/fjernet».*

Roller og tilganger i VIGO

Rollene i VIGO Opplæring er delt opp i forskjellige hovedområder definert av fylkeskommunen. Disse rollene er foreløpig ikke samkjørt for Innlandet, så det finnes tre sett roller – FK04**(Hedmark), FK05**(Oppland) FK34**(Innlandet). I oversikten revisjonen har fått tilsendt er det definert 15 ulike roller i systemet. Eksempler på roller er; *fagansvarlig, inntaksansvarlig, PPT, fagopplæring* og *inntak.* I tillegg finnes det ulike tilganger som kan knyttes til rollene. Ifølge systemansvarlig hadde Oppland og Hedmark ulikt oppsett i VIGO med ulike roller, disse ble slått sammen når de ble Innlandet fylkeskommune. I rollestrukturen er det derfor 10 roller fra Hedmark og 5 roller fra Oppland. Dette er noe de skulle ha sett på og endret, men de har ikke fått tid. Det finnes ikke administratorrettigheter ute på skolene, kun lesetilgang. Det er 83 brukere av VIGO Opplæring.

I VIGO Skole er det syv administratorer som alle er organisatorisk plassert på Inntakskontoret i fylkeskommunen. Disse syv kan opprette og endre systemansvarlige på alle grunnskoler og videregående skoler i Innlandet. Det er opprettet en systemansvarlig for VIGO Skole per skole, som videre kan opprette nye brukere på sin skole. Det finnes bare to roller i VIGO Skole; system/skoleadministrator og skolebruker. Skoleadministrator kan kun tildele skolebruker-roller. Denne rollen er fast og det er ikke mulighet for å legge til eller endre privilegier. Skolebrukere har tilgang til informasjon som elevens navn, hva eleven har kommet inn på, hva den enkelte har søkt med prioritering, personnummer og adresse. De kan også se resultater fra grunnskole og hvilken skole de har gått på. Skolebruker har kun lesetilgang i systemet.

Opprettelse og vedlikehold av brukertilganger på skolene

Det er ikke formalisert eller nedskrevet hvordan brukertilganger opprettes og vedlikeholdes i VIGO. Systemansvarlige i VIGO Opplæring beskriver at prosessen ved opprettelse av brukertilgang skjer på følgene måte:

- Systemansvarlig får beskjed fra leder om å lage bruker til nytilsatt og hvilke arbeidsoppgaver den nytilsatte skal ha.
- Får fødsels- og personnummer av nytilsatt ved at de fysisk går til nytilsattes kontor, der hjelper de også til med å installere nødvendig programvare på PC.
- Oppretter bruker-identitet og passord og haker av i systemet hva den enkelte skal ha tilgang til og gir de riktige rollene.
- Gir bruker-identitet og passord til nytilsatt.
- Nytilsatt endrer passordet ved førstegangs innlogging.

Systemansvarlige opplever at det er enkelt å holde oversikt over tilganger og at det sjelden er behov for å endre på tilgangene som er gitt. Det kan skje noen få ganger at de får beskjed fra leder om å endre tilganger eller at ansatte selv oppdager at de ikke har de nødvendige tilgangene. For å avslutte brukerkonto kan systemansvarlige velge om de skal låse kontoen eller slette. De sletter dersom vedkommende slutter og har mulighet til å låse ved eksempelvis permisjon.

Det blir kun opprettet manuelle tilganger i VIGO Skole og det er bare skoleadministrator som kan gi tilganger. I oktober/november slettes alle tilganger i systemet automatisk. Brukerkontoene ligger fortsatt i systemet, men uten tilganger. Tilgangene må fornyes manuelt hvert skoleår. For ansatte som tidligere har hatt tilgang i VIGO Skole er det nok å aktivere tilgangen igjen. For nye ansatte opprettes bruker av skoleadministrator med fødsels- og personnummer, e-post og telefonnummer.

Skoleadministratorene fortalte at de gjør endringer i tilganger dersom noen slutter eller om det starter nye med behov for tilgang. Dette gjøres manuelt da VIGO ikke er integrert med det skoleadministrative systemet VIS, «S*ystemet snakker ikke med andre system og "lever sitt eget liv" så må avslutte manuelt dersom en ansatt slutter».*

4.3.3.3 Tjenstlig behov for tilganger

Revisjonen gikk sammen med systemansvarlig i VIGO Opplæring gjennom alle tilgangene i systemet, totalt 83 brukerkontoer. Det ble i gjennomgangen avdekket at én ansatt har endret arbeidsoppgaver og at tilgangen i VIGO Opplæring skulle vært avsluttet, videre var det to ansatte som hadde sluttet som fortsatt hadde tilgang.

Det var totalt ni ansatte som hadde administratortilgang og alle rettigheter i systemet. Systemansvarlig fortalte at Hedmark og Oppland hadde hver sin oppbygging av systemet som skulle bli felles når de ble Innlandet fylke. Dette har de ikke fått gjort, men er noe som vil komme. Dette er noe av grunnen til at det er flere med administrator-rettigheter enn systemansvarlig hadde regnet med.

Tre av brukerkontoene er systembrukere og opprettet av leverandør, disse har kun lesetilgang. Systemadministrator opplever å ha liten oversikt over de som har tilgang fra PPT, da det er forskjellig ordning fra Hedmark og Oppland. Det er derfor vanskelig å si om de har riktige tilganger. Det er også noen enkeltbrukere i voksenopplæringen som har lesetilgang i VIGO, dette for å se historikk til voksne elever som ønsker å fullføre VGS.

I intervju med skoleansvarlige ble det beskrevet at det er skoleledere, rådgivere og kontorpersonell med behov for informasjon om inntatte elever, ventelister, søkerstatistikk på skolenivå og søknadsstatus, som gis tilgang til VIGO Skole. Det gis kun én tilgang/rolle og man har kun tilgang til å lese/hente ut data.

Innlogging til VIGO er tilgjengelig på internett og innlogging skjer via ID-porten for å få tilgang. Passordet har en varighet på 90 dager før det må byttes ut. Det er ikke formkrav til passord. Administratorkontoene krever ikke egne passord, da administratorrettighetene er knyttet opp til vanlig brukerkonto.

4.3.3.4 System for jevnlig kontroll og gjennomgang av tildelte tilganger i VIGO

I VIGO Opplæring og Skole kan systemadministratorene se en oversikt over alle som har tilgang samlet og per tilgangsgruppe. Logg over når og av hvem tilgang ble gitt vises ikke. Leverandøren av programmet (IST) kan på forespørsel ha logger på dette.

Det foreligger ikke noe system for jevnlig kontroll av om tildelte tilganger i VIGO Opplæring er korrekte, men systemansvarlige tar en sjekk på den aktuelle personen når noen nye starter eller når noen slutter. Systemansvarlig fortalte at det tar tid å holde tilganger oppdatert til enhver tid og at de sikkert skulle undersøkt tilgangene oftere enn hva som er eksisterende praksis. Hun fortalte at det potensielt kan ta lang tid før de oppdager om noen har vært inne i systemet, da de sjekker listen en gang pr. år (januar). Samtidig er det ikke informasjon i systemet annet enn på høst/vår.

I VIGO Skole sørger systemet for at det er minst én årlig gjennomgang av tilganger da alle tilganger sperres i oktober/november hvert år, med unntak av systemansvarlige. 1. oktober gjennomfører systemansvarlige i VIGO (IFK) en runde med sjekk av de systemansvarlige ute på skolene.

Det er i utgangspunktet fylket selv som styrer alle tilganger i VIGO, også administratorkontoer og systemansvarlige. Brukerstøtte i VIGO er konkurranseutsatt, det er per dags dato firmaet IST som er support og driftsansvarlig i VIGO.

4.3.4 REVISJONENS VURDERINGER

Tilgangsstyringen i IKT-systemet bør være innrettet i henhold til risikovurdering av informasjonsverdiene i systemet.

Informasjonssikkerhet dreier seg om å håndtere risikoen for at blant annet personopplysninger ikke blir ivaretatt på en tilfredsstillende måte. Dette gjøres ved først å identifisere hvilke personopplysninger virksomheten har og deretter gjennomføre en risikovurdering. Dersom risikovurderingen avdekker sårbarhet, må det vurderes om nye tiltak skal iverksettes for å oppnå tilfredsstillende sikkerhetsnivå for personopplysningene. Kontrollrutiner må utarbeides og følges jevnlig, for å kontrollere at tiltakene blir fulgt opp og virker etter hensikten.

Basert på mottatt informasjon fra fylkeskommunen er det ikke etablert system for gjennomføring av risikovurderinger og oppfølging av eventuelle tiltak i systemene vi har revidert. I Visma InSchool har revisjonen fått informasjon om at innføringsprosjektet sentralt, fortløpende gjør risikovurderinger når ny funksjonalitet iverksettes. Videre har fylkeskommunen selv gjennomført en vurdering av personvernkonsekvenser (DPIA) der roller og tilgangsstyring ble pekt på som områder med stor risiko. Det er gjort noen tiltak spesielt for administrativt tilsatte og prosjektet har jobbet mye med å tilpasse roller og tilganger slik at risikoen oppleves lavere nå enn ved oppstart av prosjektet. Samtidig er det en svakhet at fylkeskommunen ikke har gjennomført risikovurderinger av Visma InSchool selv. Selv om det vil være overlapp, er det sårbart dersom fylkeskommunen lener seg fullstendig på leverandørens risikovurderinger, da leverandøren naturlig nok vil se på andre risikoer enn fylkeskommunen.

I Engage ble det gjort en risikovurdering i samarbeid med alle fylkeskommunene som er en del av IKO-prosjektet, denne ble gjort i 2020 med bakgrunn i sikkerhetsbruddet i Engage. Tiltak som ble satt i verk på bakgrunn av risikoanalysen var blant annet at dataimporten fra Visma InSchool kun skulle gjelde pedagogisk ansatte. Revisjonen kan ikke se at dette tiltaket er fulgt opp, da vi i gjennomgang av tilganger i systemet så at alle ansatte (inkludert skolelever som har sendt reiseregning) får opprettet bruker i Engage. I konsekvensvurderingen som er gjort i Engage er to-faktorpålogging i Feide nevnt som et sikkerhetstiltak. Dette tiltaket er per dags dato ikke satt i verk.

I VIGO kjenner ikke systemeier og systemansvarlige til om det foreligger plan for risikovurderinger, og fylkeskommunen har ikke utarbeidet egne risikovurderinger. Det er gjort en kartlegging av informasjonen i systemet for å kartlegge omfang av personopplysninger.

Basert på informasjonen revisjonen har mottatt synes det ikke som fylkeskommunen har innrettet tilgangsstyringen i IKT-systemene i henhold til risikovurdering av informasjonsverdiene i systemet.

Fylkeskommunen bør ha implementert en formell prosess for å registrere brukere som gis tilgangsrettigheter og for forvaltning av brukertilganger i IKT-systemet. Prosessen bør omfatte hele livssyklusen til en brukerkonto. Retningslinje for tilgangskontroll og prosess for administrasjon av kontoer, tilganger og rettigheter bør dokumenteres og være kjent i virksomheten.

Nasjonal sikkerhetsmyndighet (NSM) anbefaler at virksomheter etabler en formell prosess for administrasjon av brukerkontoer, tilganger og rettigheter i IKT-systemer.

Det er leder/rektor ved de videregående skolene som er ansvarlig for at ansatte har korrekte tilganger i systemene, i praksis er det de eller den ved skolen som har ansvaret for tilgangsstyring i systemene som oppretter, endrer og sletter tilganger.

Revisjonen vurderer at Visma InSchool har etablert en formell prosess for å registrere brukere som gis tilgangsrettigheter og for forvaltning av brukertilganger, ved at de har utarbeidet en skriftlig rutine som beskriver ansvarsfordeling og hvordan tilgangsrettigheter gis, vedlikeholdes og avsluttes. Rutinen var ikke fullt iverksatt da revisjonen gjennomførte intervjuer og det var ikke alle systemansvarlige som var kjent med rutinen selv om den hadde blitt presentert for skolene en god stund før intervjuene.

I Engage og VIGO er ikke prosessen for å registrere brukere som gis tilgangsrettigheter og for forvaltning av brukertilganger dokumentert. Revisjonen vurderer at dette er en svakhet da det gjør prosessen personavhengig. Dersom systemansvarlige blir sykmeldt eller slutter vil det være krevende for nyansatte å sette seg inn i hvordan brukertilganger gis og forvaltes i systemene. I Oppfølgingsloggen opprettes tilganger av oppfølgingsansvarlig i den enkelte sak, når saken er avsluttet får oppfølgingsansvarlig varsel/påminnelse om å fjerne tilgangen.

På bakgrunn av dette vurderer revisjonen at IKT-systemene Engage og VIGO ikke har en formell prosess for å registrere brukere som gis tilgangsrettigheter og for forvaltning av tilganger. Visma InSchool har etablert en formell prosess for å registrere brukere som gis tilgangsrettigheter og for forvaltning av brukertilganger, men denne var ikke fullt implementert i gjennomføringen av intervju våren 2021. I Oppfølgingsloggen foreligger det ikke en skriftlig rutine for opprettelse av tilganger, men det tildeles tilganger kun spesifikt i den enkelte sak på bakgrunn av bekymringsmelding.

Tilgang til IKT-systemer skal være basert på tjenstlig behov.

Et av grunnkravene for å behandle personopplysninger er at opplysninger skal behandles med konfidensialitet. Konfidensialitet betyr at skoleeier og skolene skal sørge for at bare de som trenger tilgang til personopplysningene får tilgang til dem. Skoleeier skal med andre ord ha et bevisst forhold til hvem som får og hvem som ikke får tilgang (autorisasjon) til systemer som inneholder personopplysninger, og hvilken informasjon det blir gitt tilgang til. Fylkeskommunens styringsdokument for personvern og informasjonssikkerhet sier at *all tilgang til personopplysninger og systemer skal baseres på tjenstlig behov, og skal ivareta god ansvarsfordeling*.

I Visma InSchool synes det som ansvarlige for tilgangsstyring er bevisst på at ansatte ikke skal ha mer tilganger enn de har tjenstlig behov for. Samtidig hadde det vært utfordringer med at en for stor andel ansatte med administrative oppgaver ute på skolene har vært tildelt skoleleder-rolle (administratortilgang).

I Engage skal alle fag- og kontaktlærere ha tilgang, men kun til de klassene vedkommende er lærer for. Det var usikkerhet blant de som administrerte tilganger om tilganger skulle gis manuelt eller om de ble automatisk integrert med VIS, slik at det var forskjellig praksis på skolene ut fra hvilket arbeid de la ned i tilgangsstyringen. Det synes å være mange skoleadministratorer per skole som har rettigheter til å gi, endre og slette tilganger. I Oppfølgingsloggen opprettes tilganger i den enkelte sak på bakgrunn av bekymringsmelding. Revisjonen vurderer at det er mindre risiko for at det er tilganger utover tjenstlig behov da tilganger blir opprettet spesifikt til de som skal følge opp eleven i den enkelte sak.

I VIGO Opplæring hadde tre av 83 ansatte tilganger de ikke skulle hatt på grunn av endret arbeidsforhold eller at de hadde sluttet. Dette tilsvarer 4 %, noe som revisjonen vurderer er i overkant mye. Det var flere administratorer enn systemansvarlig hadde regnet med, som kan indikere at det ikke er tilstrekkelig kontroll med administratorkontoene i VIGO Opplæring.

Revisjonen vurderer at fylkeskommunen i noen grad sørger for at ansatte har tilganger basert på tjenstlig behov. Samtidig så revisjonen i gjennomgangen av tilganger at det forelå administratortilganger i større utstrekning enn det var tjenstlig behov for i systemene Visma InSchool (skoleleder-rolle) og VIGO Opplæring. Det synes også som at det er flere skoleadministratorer i Engage enn nødvendig.

Fylkeskommunen bør ha oversikt over hvem som har tilgang til de utvalgte IKT-systemene og hvem som har gitt tilgang.

Nasjonal sikkerhetsmyndighet (NSM) anbefaler at alle kontoer bør kunne spores til ansvarlig bruker og alle kontoer bør spores til en ansvarlig rolle og person som godkjente dette, jf. grunnprinsipp 2.6 *Ha kontroll på identiteter og tilganger*.

Det fremgikk i intervjuene at systemansvarlige/administratorer kan ta ut oversikt over alle ansatte med brukerkonto i systemene og se hvilken tilgang den enkelte har. Systemansvarlige/administrator i systemene kan ikke selv ta ut oversikt over når tilgangen ble gitt eller hvem som ga tilgangen, men de kan be leverandør av systemet om denne oversikten.

Selv om det er funksjonalitet i systemene for å få oversikt over hvem som har tilgang så hadde ikke fylkeskommunen en ens praksis eller rutine for å faktisk skaffe oversikt over tilganger i systemene. Fylkeskommunen har heller ikke lett tilgjengelig oversikt over hvem som har gitt tilgang uten å undersøke med leverandør av systemet.

Revisjonen vurderer på bakgrunn av dette at fylkeskommunen i mindre grad har oversikt over hvem som har tilgang til de utvalgte IKT-systemene og hvem som har gitt tilgang.

Fylkeskommunen bør ha et system for jevnlig kontroll og gjennomgang av om tildelte tilganger i IKT-systemet er korrekte.

Brukerkontoer, tilganger og rettigheter bør revideres jevnlig. Dette er spesielt kritisk med tanke på administrator-kontoer som har utvidete tilganger og rettigheter.

På bakgrunn av at fylkeskommunen har utarbeidet rutine for gjennomgang av tilganger og at den har blitt presentert skolene, vurderer revisjonen at fylkeskommunen har utarbeidet et system for jevnlig kontroll av om tildelte tilganger i Visma in School er korrekte. Revisjonen kan på bakgrunn av datamaterialet ikke vurdere om systemet for kontroll er tilstrekkelig implementert på skolene. Det er en sikkerhet i Visma InSchool ved at pedagogisk ansatte automatisk mister tilgang til elever ved skoleårets slutt. Ansatte som ikke er koblet opp til klasser/elever i timeplanen beholder tilgangen sin. Dette er ofte ansatte som har utvidete privilegier (skoleleder-rolle, administrator-rolle) det er derfor viktig med jevnlig gjennomgang av disse tilgangene. Dette var det fokus på ved skolene, men man så samtidig at det fortsatt var flere med skole-leder rolle enn de som hadde tjenstlig behov.

I Engage foreligger det ingen skriftlig rutine for gjennomgang av tilganger, systemansvarlige/administratorer har ulik tilnærming til å kontrollere tilganger i systemet. Det ble avdekket varierende praksis og risikooppfattelse blant i skolene vi så på. Enkelte kontrollerte tilganger inntil tre ganger i året i forbindelse med skolestart og midtveisvurdering 1 og 2. Andre stolte på at ansatte hadde riktige tilganger basert på opplysningene som overføres fra Visma in School. Med bakgrunn i dette vurderer revisjonen at fylkeskommunen ikke har et system for jevnlig kontroll og gjennomgang av om tilganger i Engage er korrekte. I Oppfølgingsloggen opprettes tilganger manuelt per enkeltsak og tilganger avsluttes av oppfølgingsansvarlig når saken avsluttes.

I VIGO Opplæring foreligger det ingen rutine eller system for gjennomgang av tilganger. Revisjonen vurderer at VIGO Opplæring ikke har et system for jevnlig kontroll av om tilganger er korrekte. Det er ingen skriftlig rutine for gjennomgang av tilganger i VIGO Skole. Revisjonen vurderer allikevel at det er et system for årlig gjennomgang av tilganger, da alle tilganger med unntak av systemansvarlige automatisk sperres i oktober hvert år. Videre går systemansvarlige i VIGO (ansatt i IFK) gjennom tilgangene til systemansvarlige i VIGO Skole i oktober hvert år. Gjennomgangen av systemansvarlige i VIGO Skole er ikke nedskrevet og det vil være personavhengig om dette gjennomføres, noe revisjonen vurderer som en svakhet.

Fylkeskommunen bør ha kontroll på service-/systemkontoer, utviklere og driftsbrukere og hvilke rettigheter disse kontoene har. Det bør ikke tildeles administratorrettigheter til sluttbrukere.

Fylkeskommunen skal ha kontroll på brukerkontoer som direkte eller indirekte kan kontrollere en eller flere kontoer med lavere privilegier, slik som service- og systemkontoer, utviklere og driftsbrukere. Videre bør det ikke tildeles administratorrettigheter til sluttbrukere. Oppgavene bør skilles i to kontoer, en for vanlig kontobruk og en for oppgaver som krever forhøyede rettigheter.

I VIGO er det fylkeskommunen selv som styrer alle tilganger, også administratorer og systemansvarlige. Det finnes tre systembrukere som leverandøren styrer, disse har lesetilgang. I Engage, Oppfølgingsloggen og Visma InSchool driftes løsningene i stor grad av leverandør av systemet og det benyttes ikke service-kontoer i særlig grad av fylkeskommunen selv. Revisjonen vurderer på bakgrunn av dette at fylkeskommunen synes å ha oversikt over service-kontoer som de drifter selv, men at de i mindre grad har oversikt over brukerkontoer som direkte eller indirekte kan kontrollere en eller flere kontoer med lavere privilegier, slik som service- og systemkontoer, utviklere og driftsbrukere hos leverandør.

Administratorrettigheter er knyttet opp til vanlig brukerkonto i samtlige systemer revisjonen har sett på, noe som vurderes som en svakhet. Revisjonen vurderer at det er en risiko at administratorrettigheter er knyttet opp til vanlige brukere uten at disse er ytterligere sikret. Da kan man ved å kompromittere en vanlig bruker også oppnå administrator-rettigheter.

IKT-systemets bruker- og administratorkontoer som forvalter sensitive personopplysninger, bør være beskyttet av sterk autentisering.

Datatilsynet anbefaler sterk autentisering (tofaktorautentisering/totrinnsbekreftelse/flerfaktorautentisering) ved behandling av sensitive personopplysninger og/eller personopplysninger om mange over eksterne nett, da dette gir bedre beskyttelse enn passord alene.

Visma InSchool og Engage bruker Feide for pålogging. Feide har som tidligere beskrevet mulighet til to-faktor autentisering, dette er hittil ikke iverksatt. I Feide er det bare muligheter for en brukerkonto per ansatt, noe som gjør at man ikke kan skille mellom vanlig brukerkonto og brukerkonto med administratorrettigheter. Innlogging til Visma InSchool og Engage er eksponert direkte på internett og ved å få tak i brukernavn og passord kan hvem som helst logge seg inn. Med tanke på mengden av personopplysninger som er lagret i systemene vurderer revisjonen at det er en svakhet at det ikke er satt i verk to-faktor autentisering i Feide. Spesielt dersom man ser dette i sammenheng med at det ikke er egne passord på administratorkontoer i systemene. Revisjonen vurderer på grunnlag av dette at IKT-systemer som bruker Feide som innlogging ikke i tilstrekkelig grad beskytter sensitive personopplysninger eller opplysninger om mange over eksterne nett, med sterk autentisering.

Oppfølgingsloggen behandler i større grad sensitive personopplysninger om elever enn Engage. Oppfølgingsloggen har to-faktor autentisering i form av innlogging via ID-porten. Tilsvarende skjer all innlogging i VIGO via ID-porten.

Revisjonen vurderer på bakgrunn av dette at bruker og administratorkontoer som forvalter sensitive personopplysninger i Oppfølgingsloggen og VIGO er beskyttet av sterk autentisering. Bruker og administratorkontoer som forvalter sensitive personopplysninger i Visma InSchool og Engage er ikke beskyttet av sterk autentisering.

5 KONKLUSJONER OG ANBEFALINGER

5.1 KONKLUSJONER

Med bakgrunn i vurderingene skal revisor konkludere i forhold til problemstillingene. Dersom revisor finner vesentlige avvik, skal dette komme tydelig til uttrykk i forvaltningsrevisjonsrapporten.

Problemstilling 1

Hvilke IKT-systemer behandler personopplysninger om elever i videregående opplæring og hvilke personopplysninger behandles i disse systemene?

Revisjonen har kartlagt hvilke IKT-systemer som behandler personopplysninger om elever i videregående opplæring og hvilke personopplysninger som behandles i disse systemene.

Det er omtrent 150 systemer eller applikasjoner som behandler personopplysninger om elever i de videregående skolene. Dette inkluderer digitale læremidler, pedagogiske læremidler og andre programmer/nettbaserte tjenester som krever at bruker logger på, men hvor det er svært begrenset med personopplysninger som lagres.

IKT-systemer der elevdokumentasjon registreres og behandles er VIGO, Visma InSchool, Engage, Oppfølgingsloggen, Elements, Microsoft Office 365 og LAO. Disse IKT-systemene lagrer og behandler store menger av personopplysninger om elever. Det er i hovedsak Elements, LAO, og Oppfølgingsloggen som behandler sensitive personopplysninger om elever.

LAO benyttes kun av videregående skoler i tidligere Oppland fylke. VIGO benyttes i hovedsak sentralt i fylkeskommunen ved inntakskontoret, men enkelte ansatte på skolene har tilgang til søkere ved egen skole i forbindelse med inntak.

Problemstilling 2

I hvilken grad har fylkeskommunen etablert grunnleggende retningslinjer og rutiner for tilgangsstyring?

Revisjonens hovedkonklusjon er at fylkeskommunen i mindre grad har etablert grunnleggende retningslinjer og rutiner for tilgangsstyring som bør være på plass for at tilgangsstyringen skal fungere best mulig.

Fylkeskommunen har på nåværende tidspunkt ingen overordnet retningslinje for tilgangsstyring, selv om de har på plass enkelte deler av hva en overordnet rutine bør inneholde. Det mangler tydelig ansvarsfordeling innen tilgangskontrollen og det foreligger ingen rutine for jevnlig gjennomgang av brukerrettigheter.

Feide og ID-porten benyttes for innlogging i IKT-systemer som behandler elevdokumentasjon. Fylkeskommunen har en formell passordpolicy som er innbakt i systemene og det er ikke mulig å opprette passord i strid med kravene. Selv om fylkeskommunen har implementert passordregler så finnes det ikke noe skriftlig på dette området, noe som vurderes å være en svakhet. Grunnleggende retningslinjer og rutiner for tilgangsstyring burde

også sagt noe om hvilke opplysninger og systemer som skulle vært beskyttet av to-faktorautentisering, dette mangler.

Fylkeskommunen har heller ingen aktiv sikkerhetsovervåkning i systemene for å oppdage eventuelle innbrudd i systemene. De har ikke en rutine for å følge opp databehandlers plikt til å gjennomføre sikkerhetsrevisjoner, som avtalt i databehandleravtaler, men de har i noen grad revidert databehandleravtalene.

Problemstilling 3

I hvilken grad er det etablert tilfredsstillende tiltak for tilgangsstyring i utvalgte IKT-systemer som behandler personopplysninger om elever, og i hvilken grad er disse etterlevd?

I problemstilling 3 har revisjonen undersøkt den faktiske tilgangsstyringen i IKT-systemene Visma InSchool, Engage, Oppfølgingsloggen og VIGO, basert på etablert praksis i seks videregående skoler. Revisjonens hovedkonklusjon er at fylkeskommunen i mindre grad har etablert tilfredsstillende tiltak for tilgangsstyring i utvalgte IKT-systemer som behandler personopplysninger om elever. Det er i liten grad dokumenterte og operasjonaliserte rutiner for tilgangsstyring, noe som kan synes å påvirke praksis for opprettelse, vedlikehold og avslutning av brukerkontoer ute på skolene. Av IKT-systemene som ble undersøkt er det kun Visma InSchool som har dokumentert hvordan arbeidet med tilgangsstyring skal gjennomføres.

Revisjonen har ikke fått informasjon som tilsier at tilgangsstyringen i IKT-systemene er innrettet i henhold til risikovurdering av informasjonsverdiene i systemet. Det er ikke satt i verk to-faktor autentisering i IKT-systemer som bruker Feide for innlogging, herunder Visma InSchool og Engage. Dette er systemer som behandler store mengder personopplysninger på vegne av elever i videregående skole. Videre er administratortilgang knyttet til vanlige brukerkontoer i alle systemene som er undersøkt, noe som gir større risiko dersom uvedkommende skulle få tilgang til brukerkontoen. Ved at innloggingen til IKT-systemene Engage og Visma in School er eksponert direkte på internett synes det å være en stor risiko ved at to-faktorautentisering ikke er iverksatt.

Ansvarlige for tilgangsstyring i IKT-systemene ute på skolene var opptatt av at tilganger skal være i samsvar med tjenstlig behov, noe revisjonen vurderer som positivt. Samtidig så revisjonen i gjennomgangen av tilganger at det forelå administratortilganger i større utstrekning enn det var tjenstlig behov for i IKT- systemene Visma InSchool, Engage og VIGO, noe som kan tyde på at det ikke er tilstrekkelig kontroll på administratorkontoer. Selv om det er funksjonalitet i systemene for å få oversikt over hvem som har tilgang så har ikke fylkeskommunen en ens praksis eller rutine for å faktisk skaffe oversikt over tilganger i systemene og gjøre jevnlig kontroll av om tildelte tilganger i IKT-systemene er korrekte.

5.2 ANBEFALINGER

Revisjonen har følgende anbefalinger:

1. Fylkeskommunen bør utarbeide og implementere overordnet retningslinje for tilgangskontroll basert på en overordnet informasjonsklassifisering. Retningslinjen bør inneholde følgende punkter:
    a. Tilgang tildeles i samsvar med tjenstlig behov, herunder vurdering av hvilken tilgang som er nødvendig.
    b. Rutiner for tildeling, endring, sletting og kontroll av tilganger.
    c. Rutiner for autentisering basert på graden av sensitivitet i personopplysningene og hvilken enhet pålogging skjer fra.
    d. Tildeling av rettighet til tilgang (autorisasjon) skal registreres i et register.
    e. Ansvarsfordeling innen tilgangskontrollen
2. For å sikre personopplysninger om elever i IKT-systemer som behandler sensitive personopplysninger og/eller store mengder personopplysninger, bør fylkeskommunen iverksette to-faktor autentisering i Feide.
3. Fylkeskommunen bør iverksette sikkerhetsovervåking for å oppdage sikkerhetshendelser knyttet til tilgangskontrollen.
4. Administratorprivilegier bør ha separate brukerkontoer dersom det er teknisk gjennomførbart. Som minimum bør administratorkontoer være beskyttet av to-faktor autentisering.
5. Fylkeskommunen bør sørge for jevnlig kontroll av tilganger i IKT-systemer som behandler elevdokumentasjon, spesielt tilganger med utvidete rettigheter (administratortilganger).
6. Fylkeskommunen bør innrette tilgangsstyringen i IKT-systemene i henhold til risikovurdering av informasjonsverdiene i systemet.

6 REFERANSER

Lover og forskrifter:
Lov om kommuner og fylkeskommuner (kommuneloven), LOV-2018-06-22-83.
Lov om behandling av personopplysninger (personopplysningsloven), LOV-2018-12-20-116.

Dokumenter mottatt fra Innlandet fylkeskommune:
Styringsdokument for personvern og informasjonssikkerhet, godkjent 7.4.2021.
Roller og ansvar for informasjonssikkerhet og personvern, godkjent 1.3.2021.
Arkitekturprinsipper for Innlandet fylkeskommune, august 20.
Tidlig innsats når det gjelder, IKO – en modell for systematisk frafallsforebygging
Oversikt over alle tilganger som er knyttet til de ulike rollene i Visma InSchool, datert 18. mars 2021

Andre kilder:
Datatilsynet, Personvern i skole og barnehage, samlerapport juni 2014
Datatilsynet, Virksomhetens plikter etter personvernregleverket, https://www.datatilsynet.no/rettigheter-og-plikter/virksomhetenes-plikter/
Datatilsynet, Årsrapport 2019
Datatilsynet, Årsrapport 2020
NSM, Grunnprinsipper for IKT-sikkerhet versjon 2.0, sist oppdatert 15.4.2020.
NOU 2018:14, IKT-sikkerhet i alle ledd.
Meld St. 38 (2016-2017) IKT-sikkerhet. Et felles ansvar.
ISO 27001:2017
Oppland Arbeiderblad «PYSA-banden hadde administrator-ID til Østre Totens datasystemer» avisutklipp av 27.08.2021.
KS, Orden i eget hus, kommunedirektørens internkontroll versjon 3, april 2020

7 VEDLEGG KOMMUNEDIREKTØRENS UTTALELSE

Innlandet fylkeskommune

INNLANDET REVISJON IKS
Postboks 153

2626 LILLEHAMMER

Offl. § 5 1. ledd

Deres ref:	Vår ref:	Dato:
2021-1300	2020/47069-8 Yngve Nordseng	09.12.2021

Fylkeskommunedirektørens uttalelse til forvaltningsrevisjonsrapport Elevdokumentasjon og tilgangsstyring i vgs

Viser til oversendelsesbrev og rapportutkast mottatt 17.11.2021 samt korrigert rapportutkast mottatt 01.12.2021. Fylkeskommunedirektørens uttalelse sorteres med utgangspunkt i spørsmålene fra oversendelsesbrevet.

1. **Har informasjonen om prosjektets formål og gjennomføring vært god nok?**
   Informasjonen om formål og plan for gjennomføring av forvaltningsrevisjonsprosjektet oppleves som god. Fylkeskommunedirektøren har ingen bemerkninger til dette punktet.

2. **Har dere kommentarer til prosjektets metode, anvendte kilder eller beskrivelse av fakta?**
   Valg av metode og anvendte kilder vurderes som hensiktsmessig sett opp mot prosjektets formål. Når det gjelder beskrivelse av fakta er det gitt anledning til å kvalitetssikre dette i prosessen. Fylkeskommunedirektøren opplever det som utelukkende positivt at revisjonen har knyttet til seg ekstern ekspertise for å kvalitetssikre revisjonskriterier, metode og vurderinger.

   Fylkeskommunedirektøren har to mindre bemerkninger til fakta i rapportutkastet:

   - Storsteigen videregående skole har til sammen ca. 120 elever på to skolesteder, ikke 62 elever som beskrevet i rapporten.
   - Enheten Digitale tjenester i Kompetanse og tannhelse ble opprettet 1. mai 2021. Enhetsleder var derfor ikke involvert i dette prosjektet før i avslutningsfasen.

3. **Har dere kommentarer til revisjonskriteriene som ligger til grunn for våre vurderinger og konklusjoner?**
   Fylkeskommunedirektøren har ingen kommentarer til revisjonskriteriene, men legger

Postadresse: Postboks 4404 Bedriftssenteret 2325 Hamar
Besøksadresse: Innlandet fylkeskommune Parkgata 64 Hamar
Telefon: +47 62 00 08 80
E-post: post@innlandetfylke.no
Internett: www.innlandetfylke.no
Org.nr.: 920717152

til grunn en tolkning av kulepunkt 4 under problemstilling 2 i avsnitt 3.1.5: *"Fylkeskommunen bør ha et system for brukeridentiteter og passord, all tildeling av rettigheter til tilgang bør registreres i et register"*. Dette tolkes som at det er autorisasjonen og ikke selve tilgangene det henvises til, slik at faktiske tilganger kan kontrolleres mot et autorisasjonsregister.

Fylkeskommunedirektøren opplever det som positivt at kapittel 3 beskriver kildene som ligger til grunn for valg av de konkrete revisjonskriteriene.

4. **I hvilken grad oppfattes rapporten som nyttig?**
   Fylkeskommunedirektøren opplever rapporten som nyttig i det videre arbeidet med informasjonssikkerhet, både konkret knyttet til elevdokumentasjon og på mer generelt grunnlag.

5. **Har dere kommentarer til rapportens oppbygning og språk?**
   Rapportens oppbygning og språk er generelt bra, men fylkeskommunedirektøren kunne ønsket at særlig anbefalingene, men også revisjonskriteriene, var nummerert i stedet for opplistet med kulepunkter. Dette for å sikre korrekte henvisninger ved bl.a. tiltaksoppfølging.

6. **Hva er kommunedirektørens samlede vurdering av revisjonsrapportens vurderinger, konklusjoner og anbefalinger?**
   Fylkeskommunedirektørens samlede vurdering er at revisjonsrapporten gir et representativt situasjonsbilde av problemstillingene på revisjonstidspunktet, med unntak av revisjonsrapportens vurdering av manglende aktiv sikkerhetsovervåking i punkt 5.1. De utvalgte systemene som er revidert med tanke på tilgangsstyring; Vigo, Engage inkl. Oppfølgingsloggen og Visma InSchool, driftes alle av eksterne leverandører/databehandlere. I databehandleravtalene som er inngått med disse leverandørene stilles det krav til sikkerhetsovervåking og umiddelbar varsling av Innlandet fylkeskommune ved eventuelle sikkerhetsbrudd.

   Når det gjelder anbefaling 4 om separate brukerkontoer for administratorprivilegier, vil fylkeskommunedirektøren påpeke at det ikke er teknisk mulig å separere bruker- og administratorkonto for løsninger som utelukkende benytter eksterne autentiseringsløsninger som Feide eller ID-porten.

   Fylkeskommunedirektøren kan informere om at iverksetting av tiltak er påbegynt for følgende anbefalinger:

   Anbefaling 1:
   Arbeidet med overordnet retningslinje for tilgangskontroll forventes ferdigstilt tidlig i 2022.

   Anbefaling 2:
   Som beskrevet i rapportutkastet er det tekniske årsaker til at implementering av dette har blitt utsatt. Teknisk løsning er nå på plass, men det gjenstår testing før utrulling kan iverksettes. Dette forventes ferdigstilt i løpet av januar 2022.

Fylkeskommunedirektøren vil sørge for at oppfølgingstiltak for de øvrige anbefalingene legges inn i planene for informasjonssikkerhetsarbeidet i 2022.

Fylkeskommunedirektørens vurdering av hvordan den endelige rapporten skal presenteres i forhold til offentlighet

Fylkeskommunedirektøren ber om at dataflytskissen under punkt 4.2.1.1 unntas offentlighet. Skissen alene inneholder ikke tilstrekkelig informasjon for å kunne skaffe uautorisert tilgang til systemene, men den vil kunne bidra med vesentlig informasjon i forbindelse med kartlegging av fylkeskommunens informasjons- og sikkerhetsarkitektur.

Fylkeskommunedirektøren ber også om utsatt offentlighet for hele rapporten inntil tiltak knyttet til anbefaling 2 er ferdigstilt. Dette fordi oppmerksomhet rundt dette punktet kan stimulere til uønsket aktivitet eller forsøk på uautorisert tilgang.

Ut over disse punktene vurderer ikke fylkeskommunedirektøren at det er grunnlag for at hele eller deler av rapporten skal unntas offentlighet.

Med vennlig hilsen

Tron Ole Bamrud
Fylkeskommunedirektør

Dette dokumentet er elektronisk godkjent og sendes uten signatur.