Krav til en vertsorganisasjon i Feide

Veiledning |

Om Senter for IKT i utdanningen

Senter for IKT i utdanningen ble opprettet 1. januar 2010 og er underlagt Kunnskapsdepartementet. Senteret skal bidra til å iverksette regjeringens politikk innenfor grunnopplæringen, barnehageområdet og lærer- og førskolelærerutdanningen, og er en sammenslåing av flere tidligere nasjonale initiativ; ITU, Uninett ABC og Utdanning.no.

Dette dokumentet er en del av senterets dokumentbibliotek og er derfor løftet frem under senterets samlede profil med ny forside.

Rettigheter

Senter for IKT i utdanningen // Publisert 2008, revidert 2011, trykket oktober 2012

Forord

Om FEIDE

Feide står for Felles Elektronisk IDEntitet og er Kunnskapsdepartementets satsing på enhetlig identitetsforvaltning i utdanningssektoren, både for grunnopplæringen og for høyere utdanning.

Senter for IKT i utdanningen har ansvar for å veilede skoleeiere ved innføringen av Feide i grunnopplæringen. Veiledningen er et gratis og leverandørnøytralt tilbud til alle skoleeiere i Norge.

Arbeidet med utvikling av Feides tekniske løsning, juridiske aspekter og annet Feide-arbeid koordineres av den sentrale Feide-organisasjonen i UNINETT AS. Les mer om Feide på **www.feide.no**

Om denne veiledningen

Veiledningen retter seg mot skoleeiere som skal innføre Feide. Feide stiller krav til organisasjoner som ønsker å knytte seg til Feides innloggingstjeneste. Veiledningen tydeliggjør kravene Feide stiller, og gir samtidig anbefalinger om hvordan organisasjonen kan oppfylle kravene. Ulike krav kan være relevante for ulike deler av organisasjonen.

DEL I (kapittel 1 og 2)

omtaler krav som gjelder hele organisasjonen.

Del II (kapittel 3 og 4)

omtaler krav til teknisk løsning og organisering.

Del III (kapittel 5)

beskriver rutiner rundt søknadsprosessen for å bli Feide-godkjent.

Bakerst finner du en ordliste, samt vedlegg som teksten henviser til.

Innholdsfortegnelse

Innledning

En vertsorganisasjon er i Feide-sammenheng en skoleeier, dvs. en kommune, fylkeskommune, høgskole eller lignende. En Feide-vertsorganisasjon tildeler Feide-navn til sine tilknyttede personer og håndterer autentiseringsinformasjon og brukerattributter.

Organisasjoner som ønsker å knytte seg til Feides innloggingstjeneste og dermed bli vertsorganisasjon, må tilfredsstille en del krav. Kravene kan grupperes i:

- krav til behandling av personopplysninger
- krav om innføring av IKT-reglement
- krav til den tekniske løsningen
- krav om førstelinjesupport

Henvisning til krav fra Feide-kontrakten eller kontraktens vedlegg er angitt med store bokstaver og klammeparentes.

- [KON1] betyr at kravet finnes i Feide-kontraktens del 1: *«Avtalevilkår»*.
- [KON2] betyr at kravet finnes i Feide-kontraktens del 2: *«Beskrivelse av Feide og hver av partenes ansvarsområder»*.
- [VED1-1] betyr at kravet finnes i Feide-kontraktens vedlegg 1-1: *«Feide systemarkitektur»*.

Anbefalinger om hvordan krav skal oppfylles, er angitt med vanlig skrift.

LENKER TIL RELEVANT INFORMASJON

Formelle dokumenter som benyttes i søknader og kontrakter i forbindelse med Feide, er samlet på www.feide.no. Her er nettadresser til dokumenter som det henvises til i veiledningen:

Søknadsskjema for vertsorganisasjoner og kontraktens del I (Avtalevilkår) og II (Beskrivelse av partenes ansvarsområder): http://www.feide.no/avtaler-vertsorganisasjoner

- Kontraktens vedlegg 1.1 «Feide systemarkitektur» og 1.2 «Feides informasjonsmodell for grunnopplæringa» (Bruk av norEdu* Object Class Spesification v.1.5 for grunnopplæringa): http://www.feide.no/teknisk
- Priser for vertsorganisasjoner: http://www.feide.no/priser-vertsorganisasjoner
- Temaheftet «Datavask og rutiner - beste praksis»: http://www.uninettabc.no/temahefter/datavask
- Temaheftet «Brukernavn og passord - beste praksis»: http://www.uninettabc.no/temahefter/brukernavn
- Forslag til felles IKT-reglement: http://www.uninettabc.no/publikasjoner/

KAP. 1

Krav til behandling av personopplysninger

En personopplysning er en opplysning knyttet til en enkeltperson. Eksempler på personopplysninger er navn, adresse, telefonnummer og bilder. Identitetsforvaltning handler om å håndtere personopplysninger for å identifisere personer og for å kontrollere deres tilgang til ulike ressurser. Feide er Kunnskapsdepartementets satsing på en enhetlig identitetsforvaltning for utdanningssektoren, og bygger på tillit mellom Feide-organisasjonen sentralt og tilknyttede vertsorganisasjoner. Feide er avhengig av at en vertsorganisasjon har god kontroll på sin lokale identitetsforvaltning:

Krav 1.1: *Feide krever at organisasjonen har skriftlige retningslinjer for identitetsforvaltning [VED1-1, kap. 7].*

Retningslinjene bør blant annet angi

- hvem som skal tildeles elektroniske identiteter i organisasjonens IKT-infrastruktur, for eksempel elever, lærere, andre ansatte og andre personer som er tilknyttet organisasjonen.
- hvordan identiteten skal opprettes.
- hvordan identiteten skal vedlikeholdes.
- hva identiteten skal brukes til.
- når identiteten skal termineres.

Å sørge for kontroll på den lokale identitetsforvaltningen angår hele organisasjonen.

1.1 TILSYN OG REGELVERK

Feide innebærer at hver enkelt organisasjon har det fulle behandlingsansvaret for personopplysninger om sine brukere. Dermed er hver organisasjon ansvarlig for at deres behandling av slike opplysninger skjer i henhold til norsk lovverk.

Følgende krav er inkludert i Feide-kontrakten:

Krav 1.2: *Organisasjonen plikter å sørge for at all behandling av personopplysninger utføres etter gjeldende regelverk [KON2, kap. 1.3].*

Krav til beskyttelse av data og til personvern er regulert av norsk lov. Flere deler av norsk lovgivning er relevante i forhold til behandling av personopplysninger, blant annet personopplysningsloven, helseregisterloven, forvaltningsloven og offentlighetsloven. Særlig viktig er personopplysningsloven, som skal beskytte den enkelte mot at personvernet blir krenket gjennom behandling av personopplysninger. Se lovteksten her: http://www.lovdata.no/all/hl-20000414-031.html.

Personopplysningslovens § 31-35 omhandler melde- og konsesjonsplikt. Her heter det blant annet at elektronisk behandling av personopplysninger skal meldes til Datatilsynet. Videre heter det at behandling av sensitive personopplysninger krever konsesjon fra Datatilsynet.

Følgende krav er derfor hentet fra personopplysningsloven og inkludert i Feide-kontrakten:

Krav 1.3: *Organisasjonen er ansvarlig for behandling av personopplysninger. Organisasjonen er herunder meldings- og konsesjonsansvarlig overfor Datatilsynet [KON1, kap. 9.2].*

Les mer om melde- og konsesjonsplikt på Datatilsynets nettsted: http://www.datatilsynet.no/templates/article____215.aspx.

1.2 DATAKVALITET

Feide bygger på gjensidig tillit mellom tilknyttede vertsorganisasjoner, og forutsetter at samtlige organisasjoner leverer data av god kvalitet:

Krav 1.4: *Feide krever at organisasjonen til enhver tid leverer konsistente og oppdaterte data [VED1-1, kap. 4.1].*

Krav 1.5: *Feide krever at organisasjonen har tilstrekkelig kvalitet på sine data i de autoritative datakildene [KON2, kap. 1.3].*

Krav 1.6: *Feide krever at organisasjonen kan verifisere at rutiner for håndtering av de autoritative datakildene er gode og vedlikeholdes slik at det bevares og leveres data av best mulig kvalitet [VED1-1, kap. 6].*

Vi anbefaler følgende tiltak for å oppfylle kravene ovenfor:

- Sikre god orden i alle kildesystemer.
- Innfør rutiner for å opprettholde god datakvalitet i kildesystemene.
- Følg opp rutinene kontinuerlig for å sikre fortsatt god datakvalitet.

Disse tre temaene behandles i hvert sitt underkapittel (kap. 1.2, 1.3 og 1.4).

1.2.1 Rydd opp i alle kildesystemer

Kildesystemer skal inneholde korrekt, konsistent og oppdatert informasjon. Oppryddingen omfatter å kontrollere alle kildesystemer, og å rydde og korrigere hvis det finnes feil eller inkonsistens i informasjonen. Husk at denne opprydningen bør gjelde hele organisasjonen, og ikke først og fremst IT-avdelingen.

Arbeidet med å rydde i kildesystemene bør starte allerede før man går i gang med å lage og innføre nye rutiner. Samtidig er rutiner og regler til god hjelp under ryddingen. Opprydding og innføring av rutiner (kapittel 1.3) er derfor ikke uavhengige aktiviteter, men kan med fordel utføres parallelt.

Hvis organisasjonen ikke allerede har ryddet i systemene og kartlagt hvor personopplysningene behandles, vil det å sikre korrekt, konsistent og oppdatert informasjon være den største jobben ved å innføre Feide.

1.2.2 Kartlegg hvor personopplysninger finnes

Det er viktig å ha kontroll på hvilke personopplysninger som lagres hvor. De første viktige stegene på vei mot ryddige kildesystemer er å

- kartlegge hvilke personregistre som finnes for elever/studenter, lærere og andre ansatte.
- kartlegge hvilke tjenester som benyttes på de ulike skolene, både lokale og sentrale.
- kartlegge hvilke personopplysninger som finnes i de forskjellige personregistrene.
- kartlegge hvilke personopplysninger som benyttes av de forskjellige tjenestene.
- bestemme hva som skal være autoritativt kildesystem for hver personopplysning om ulike persontyper (elever/studenter, lærere, andre).

Kartleggingen bør være så grundig som mulig, og den bør omfatte alle personregistre og tjenester. Kartleggingsprosessen viser sannsynligvis at personopplysninger behandles på langt flere steder enn antatt.

1.2.3 Kontroller alle personopplysninger

Sørg for å sikre at personopplysningene som behandles, er korrekte. Oppdaterte kildesystemer oppnås ved å

- fjerne utdatert informasjon
- fjerne duplisert informasjon
- sørge for at all eksisterende informasjon følger de nye rutinene

Hensikten med en slik kartlegging og kontroll er å sørge for at personopplysninger behandles færrest mulig steder, og dermed redusere risikoen for feil. Organisasjonen må vite hvor ulike personopplysninger lagres, endres og hentes fra, og behandlingen av opplysninger må følge eksisterende rutiner.

1.3 INNFØRING AV RUTINER

Orden i kildesystemene forutsetter rutiner for hvordan personopplysninger skal behandles. Personopplysningslovens § 13-14 krever at rutiner for behandling av personopplysninger dokumenteres, og at dokumentasjonen er tilgjengelig for alle som jobber med personopplysningene eller systemene disse behandles i,

og dessuten for Datatilsynet og Personvernnemnda. Det er viktig at alle som jobber med personopplysninger, er kjent med de etablerte rutinene. Like viktig er det at alle følger dem.

Vi anbefaler at rutinene omfatter

- registrering av personopplysninger
- regler for bruk av datafelter
- endring av personopplysninger
- sletting av personopplysninger

Disse fire temaene behandles i hvert sitt underkapittel (kapittel 1.3.1–1.3.4).

Vedlegg 2 viser sjekklisten Feide bruker for å gjennomgå vertsorganisasjonenes systemer. Sjekklisten sikrer at rutiner som sørger for korrekte og oppdaterte data, er på plass. Les mer i temaheftet «Datavask og rutiner - beste praksis».

1.3.1 Registrering av personopplysninger

En viktig forutsetning for ryddige kildesystemer er at de som legger inn nye personer i systemene, følger samme regler. Alle som jobber med registrering av personopplysninger, må derfor være enige om følgende:

Når skal en person registreres?
Registrering kan for eksempel skje ved ansettelse/inntak, eller ved første arbeids-/skoledag. Uansett må registreringen utføres konsekvent og likt av alle.

Hvilken informasjon skal legges inn om en person?
Feide krever tilgang til et minimum av informasjon om alle tilknyttede brukere. Et eget Feide-skjema definerer et standardsett attributter for hver bruker. Se «Feides informasjonsmodell for grunnopplæringa» for oversikt over Feide-attributtene.

I tillegg vil ofte lokale tjenester som er knyttet til identitetsforvaltningssystemet, kreve en del informasjon utover de obligatoriske Feide-attributtene. Slik ekstra informasjon må også registreres i systemene.

Hvor kommer informasjonen fra?
Bli enige om hvor informasjonen som skal inn i kildesystemene, skal hentes fra. Informasjonen kan for eksempel hentes fra elektroniske systemer, fra skriftlige skjemaer, eller som muntlige beskjeder.

Hvilken kvalitet har informasjonen?
Alle må kunne stole på at kildene for informasjon er korrekte og oppdaterte. Sørg derfor for at informasjonen til enhver tid holder best mulig kvalitet.

Svarene på disse spørsmålene må inngå i organisasjonens rutiner for behandling av personopplysninger.

1.3.2 Regler for bruk av datafelter

Innføring av Feide innebærer at informasjon må flyte mellom ulike systemer. Dermed oppstår det et behov for samkjøring av informasjon. Det betyr at hvert enkelt system ikke lenger kan bruke samme informasjonsfelter på hver sin særegne måte. Systemer som utveksler informasjon, må bruke samme felter på samme måte.

Mange systemer inneholder såkalte fritekstfelter, det vil si felter hvor en i praksis kan registrere og legge inn hva som helst. Siden det ikke er tekniske begrensninger for hvilken informasjon som ligger i disse feltene og på hvilket format, er praksis for hvordan slike felt brukes, svært varierende. Det må derfor innføres konsistente regler for hvordan feltene fylles ut, slik at informasjonen i fritekstfeltene ikke går tapt. Spesielt viktig blir dette når informasjonen flyter på tvers av systemer.

For å sikre at datafelter brukes på en konsistent måte, må alle være enige om følgende:

Hvilke felter skal være obligatoriske å fylle ut?
Det må være regler for hvilken informasjon som må foreligge om brukere, organisasjon og tilhørigheter.

Hvilke felter skal være valgfrie å fylle ut?
På samme måte må det finnes regler for hvilken informasjon som kan foreligge utover den obligatoriske.

Hvilke felter skal ikke fylles ut?
Det må også finnes regler for hvilke felter som eventuelt ikke skal fylles ut, for eksempel dersom feltene skal fylles med informasjon fra andre kilder.

Skal et felt kunne inneholde én eller flere verdier?
Det kan for eksempel være tillatt med flere registrerte telefonnumre per bruker, men bare ett fødselsnummer.

Hvilken informasjon skal ligge i hvilket felt?
Det kan for eksempel være aktuelt å tillate at telefonnummerfeltet fylles ut med mobilnummer dersom det ikke finnes noe annet telefonnummer.

Hvilke felter skal inneholde tall, og hvilke skal inneholde tekst?
Selv om et datafelt aksepterer flere typer data, er det ikke sikkert at all tekst fanges opp av grensesnittene som sender informasjonen videre. Dersom det legges kommentarer i et telefonnummerfelt som tillater bokstaver, kan denne informasjonen gå tapt i videre overføring.

Etter hvilke standarder eller normer skal hvert felt fylles ut?
Typiske data det er viktig å beslutte standarder for, er navn (for eksempel fornavn, mellomnavn, etternavn) og telefonnummer (for eksempel +xx yyyyyyyy). Fødselsnummer følger nasjonale standarder.

Hvordan brukes roller?
Roller må brukes på en konsistent måte. Skal for eksempel en person kunne være lærer og foresatt samtidig? Hvilke regler skal da gjelde for valg av primærrolle?

Dette er viktige forhold som bør avklares når organisasjonen lager regler for bruk av datafelter. I tillegg må dere tenke gjennom om organisasjonen har behov for særskilte datafelter.

1.3.3 Endring av personopplysninger

En annen forutsetning for ryddige kildesystemer er at alle følger de samme reglene når personopplysninger skal endres. Alle endringer gjøres i kildesystemene, som videre oppdaterer andre tilknyttede systemer. For å opprettholde god datakvalitet, er det viktig at endringer i kildesystemene gjøres riktig og konsekvent. Alle som kan gå inn og endre personopplysninger, må derfor være enige om følgende:

Hvordan meldes endringer?
Det finnes flere alternativer for å melde endringer: via elektroniske selvregistreringssystemer, skriftlige skjemaer eller muntlige beskjeder.

Hvem kan initiere endringer av forskjellig type informasjon?
Vanligvis vil en person selv kunne melde fra om nytt telefonnummer, mens endring av rolle fra «elev» til «ansatt» vil kreve at noen andre melder fra.

Hvem har ansvar for å gjøre endringene?
Det bør oppnevnes én eller flere ansvarlige for hvert system som inneholder personopplysninger.

Hvor lang tid skal det gå fra en endring blir meldt inn til den blir registrert i et kildesystem?
Det bør settes et maksintervall som sikrer at informasjonen til enhver tid er tilstrekkelig oppdatert.

Hvor kommer den nye informasjonen fra?
Informasjon kan komme fra blant annet elektroniske systemer, skriftlige skjemaer eller muntlige beskjeder.

Hvilken kvalitet har den nye informasjonen?
Alle bør kunne stole på at kildesystemene inneholder korrekt og oppdatert informasjon. Dersom endringene som legges inn i dette kildesystemet, spres til andre systemer, er det viktig at informasjon endres kun i kildesystemet, og at den herfra spres videre til andre aktuelle systemer.

Svarene på disse spørsmålene må inngå i organisasjonens rutiner for behandling av personopplysninger.

1.3.4 Sletting av personopplysninger

Ryddige kildesystemer forutsetter at alle som sletter personopplysninger, utfører slettingen etter samme regler. Alle må være enige om følgende:

Hvordan meldes en sletting?
Slettingen kan meldes gjennom for eksempel skriftlige skjemaer eller muntlige beskjeder. I tillegg kan summen av flere informasjonselementer vise at en bruker ikke lenger er aktiv. For eksempel skal en bruker som kun har elevtilknytning, men ingen aktive fag, ikke lenger være aktiv elev.

Hvem kan initiere en sletting av informasjon?
Sletting av informasjon er aktuelt når en elev eller ansatt slutter og ikke lenger er tilknyttet organisasjonen. Det må være avklart hvem som gir beskjed om slike hendelser.

Hvem har ansvar for å gjøre slettingen?
Det bør oppnevnes én eller flere ansvarlige for hvert system som inneholder personopplysninger.

Hvor lenge etter at en person har sluttet, slettes personopplysninger?
Lovkrav og retningslinjer kan bestemme at noe informasjon må oppbevares i et bestemt tidsrom etter at personen har sluttet i organisasjonen. Dette må organisasjonen ha klart.

Hvordan forsikrer en seg om at en sletting faktisk skal gjennomføres?
Det må defineres hvilken informasjon som må være på plass før slettingen utføres.

Skal en person kunne komme tilbake til organisasjonen og få tilbake den samme informasjonen?
I så fall – i hvor lang tid skal det være mulig?

Svarene på disse spørsmålene må inngå i organisasjonens rutiner for behandling av personopplysninger.

1.3.5 Verifisering av registrert informasjon

For å øke sannsynligheten for at registrerte personopplysninger er korrekte, bør det innføres rutiner som verifiserer all registrert informasjon. Dette kan gjøres ved hjelp av selvregistreringssystemer, der brukeren med jevne mellomrom selv må verifisere at registrerte opplysninger er korrekte. I tillegg bør det finnes rutiner som sikrer at informasjonen raskt kan endres dersom den ikke er korrekt.

Feide-brukere kan logge seg inn på http://innsyn.feide.no for å verifisere registrert informasjon i organisasjonens lokale Feide-katalog.

1.4 KONTINUERLIG OPPFØLGING AV RUTINER

Det viktigste tiltaket for å sikre kontinuerlig oppfølging av rutinene, er å gi de som jobber med kildesystemene, tilstrekkelig informasjon og opplæring. Alle som jobber med kildesystemene, må gjøres kjent med eksisterende rutiner. Det er lurt å understreke årsaken til at rutinene innføres og følges, og å gjøre alle klar over konsekvensene av ikke å vedlikeholde kildesystemene. Svikt i rutinene kan føre til at kildesystemene ikke lenger inneholder korrekt, konsistent og oppdatert informasjon. Feil i kildesystemene spres så videre til andre systemer som kildesystemene oppdaterer.

1.5 KRAV OM BRUK AV ROLLER

En rolle definerer et sett av rettigheter, oppgaver, ansvar, forpliktelser eller lignende som kan tildeles en aktør, som regel en person. Feide krever at enhver Feide-bruker har minst én definert rolle/tilknytning til sin organisasjon. Brukeren kan ha flere roller, og kan i så fall ha én av dem som sin primære rolle. Det er viktig at roller brukes konsekvent:

Krav 1.7: *De roller og former for tilknytning som brukere kan ha til organisasjonen, må være klart definert. Organisasjonen må sikre at interne prosedyrer tildeler og bruker roller/tilknytning* konsistent*. Alle Feide-brukere har en eller flere tilknytninger til sin vertsorganisasjon, valgt fra et lite, men fleksibelt sett. En av tilknytningene skal være identifisert som den primære [VED1-1, kap. 6].*

Eksempler på roller er «elev» og «ansatt». LDAP-skjemaet for Feide, nordEdu* Class Specification, definerer roller som benyttes i Feide. Atributtet eduPersonAffiliation er obligatorisk og forhåndsdefinert. Organisasjonen kan også selv definere spesifikke roller ved hjelp av attributtet eduPersonEntitelment. I autentiseringstjeneren må alle roller som defineres i organisasjonen, avbildes til en av rollene i norEdu*-spesifikasjonen. Vi anbefaler derfor organisasjonene å holde seg til de rollene som er brukt i denne spesifikasjonen.

For mer informasjon om bruk av roller henvises til dokumentet «Feides informasjonsmodell for grunnopplæringa». Se dette dokumentet for beskrivelse av hvordan atributtene eduPerson-Affiliation og eduPersonEntitelment brukes i grunnopplæringen.

1.6 KRAV OM SKRIFTLIG DOKUMENTASJON

Personopplysningsloven krever at organisasjoner som behandler personopplysninger, skal dokumentere denne behandlingen. Med hjemmel i personopplysningsloven kan Datatilsynet kreve innsyn i skriftlig dokumentasjon av behandlingen av personopplysninger. UNINETT kan også be om tilgang til slik dokumentasjon. Følgende krav er altså et krav om at UNINETT kan be om innsyn i dokumentasjon som allerede bør finnes:

Krav 1.8: *UNINETT kan når som helst kreve å få skriftlig dokumentert behandling av personopplysninger som er inkludert i Feide-skjema og som organisasjonen har utstedt Feide-navn for [KON2, kap. 1.3].*
Denne dokumentasjonen må som et minimum omfatte:

a. Informasjon om organisasjonens hjemmelsgrunnlag. Hjemmel, eller rettslig grunnlag for behandling av personopplysninger, finnes i personopplysningsloven § 8. Alternative hjemler er samtykke, krav om registrering i lov, eller såkalt nødvendighet.

b. Informasjon om hvordan grunnkravene overholdes for
   - behandling av personopplysninger (se personopplysningslovens kapittel II)
   - ivaretakelse av de registrertes rettigheter (se personopplysningslovens kapittel III og IV)
   - krav til informasjonssikkerhet (se personopplysningslovens § 13)

c. Informasjon om hvordan reglene for innsyn og annen informasjon om behandlingen overholdes, altså informasjon om hvordan organisasjonen ivaretar enhver brukers rett til innsyn, som beskrevet i personopplysningslovens § 18.

KAP. 2

Krav om innføring av IKT-reglement

Et IKT-reglement inneholder prinsipper og normer for hvordan IKT skal anvendes. Feide krever at enhver tilknyttet vertsorganisasjon har etablert et slikt reglement:

Krav 2.1: *Feide krever at vertsorganisasjoner holder sine brukere ansvarlig for å respektere retningslinjer for akseptabel bruk av IKT-utstyr [VED 1-1, kap. 7].*

Krav 2.1 oppfylles ved at det innføres IKT-reglement for elever og ansatte. Vi anbefaler å vurdere forslag til felles IKT-reglement som utgangspunkt for IKT-reglement for organisasjonen. Dette forslaget til IKT-reglement for utdanningssektoren er utarbeidet i samarbeid med Trondheim kommune og Senter for rettsinformatikk ved Universitetet i Oslo. Reglementet kan tilpasses og anvendes av ulike institusjoner i sektoren.

Det er viktig at samtlige brukere gjøres kjent med IKT-reglementet:

Krav 2.2: *Organisasjonen plikter å gjøre alle sine brukere kjent med gjeldende IKT-reglement [KON2, kap. 1.6].*

En vanlig måte å gjøre dette på, er å kreve at alle brukere skal signere på at de har lest og forstått IKT-reglementet før de får tilgang til datasystemene. Flere organisasjoner har selvbetjeningstjeneste for aktivering av brukerkonto. Da kan brukerne gjøres kjent med IKT-reglementet ved at de godtar reglementet idet de aktiverer kontoen. I tillegg bør reglementet henges opp godt synlig overalt der datasystemene er i bruk, samt være lett tilgjengelig på organisasjonens nettsider. Organisasjonen må selv håndheve at brukerne overholder regler i IKT-reglementet.

Krav 2.3: *Organisasjonen har ansvar for at godtatte regler for akseptabel bruk blir håndhevet. Hva som er akseptabel bruk, må fastsettes av organisasjonen og gjøres kjent for brukerne [VED1-1, kap. 4].*

For å definere hva som er akseptabel bruk av IKT-systemene, anbefaler vi å ta utgangspunkt i utkast til felles IKT-reglement som nevnt over.

Feide krever at vertsorganisasjonen følger opp sine brukere:

Krav 2.4: *Organisasjonen plikter å følge opp klager på brukere som opptrer i strid med regelverk. Slike brukere kan bli fratatt adgang til Feide-innlogging [KON2, kap. 1.7].*

Feide bygger på gjensidig tillit mellom alle tilknyttede vertsorganisasjoner. Feide forutsetter at hver organisasjon har et godt IKT-reglement, og at organisasjonen følger opp at brukere overholder reglementet.

DEL
II

KAP. 3

Krav til teknisk løsning

I Feide-arkitekturen står Feide for den sentrale innloggingstjenesten, mens hver organisasjon autentiserer sine brukere:

Krav 3.1: *Organisasjonen skal tilby autentisering av egne brukere [VED1-1, kap. 4.2.1].*

Dette gjøres ved å tilfredsstille kravene om kildesystem, brukeradministrativt system (BAS) og autentiseringstjener (AT).

3.1 KILDESYSTEM

Feide er en elektronisk identitetsforvaltning som krever at nødvendige personopplysninger foreligger i elektronisk form. Derfor må også organisasjonens kildesystemer være elektroniske:

Krav 3.2: *Underlagsdata for LDAP-katalogen må være i elektronisk form [VED1-1, kap. 6].*

Det er viktig at vedlikehold av informasjon ikke dupliseres. For hvert informasjonselement, for eksempel etternavn, må det være klart hvilket kildesystem det hentes fra for en bestemt type person. Dersom informasjon hentes fra flere kildesystemer, må prioritering være definert for hvert informasjonselement. Alle endringer skal skje i kildesystemer:

Krav 3.3: *Organisasjonen definerer ett kildesystem som autoritativt for hvert personattributt: For hvert attributt, for eksempel «navn» eller «telefonnummer», finnes én definert autoritet. Alle andre steder der samme attributtverdi benyttes, betraktes som kopier. Oppstår det tvil om korrekt verdi for et attributt, er verdien fra den autoritative kilden bestemmende. I organisasjoner med ulike grupper brukere, for eksempel studenter og ansatte, kan autoritativ kilde være ulik for hver gruppe [VED1-1, kap. 6].*

En forutsetning for å levere korrekte, konsistente og oppdaterte data er at organisasjonen rydder opp i samtlige kildesystemer. Rutiner for håndtering av de autoritative kildesystemene må sørge for at det til enhver tid leveres data av best mulig kvalitet. Dette er en kontinuerlig «ryddeprosess»:

Krav 3.4: *Rutiner for håndtering av hvert autoritative kildesystem må, om nødvendig, tilpasses slik at det bevares og leveres data av best mulig kvalitet. Dette er en kontinuerlig pågående prosess [VED1-1, kap.6].*

Les mer om hvordan opprydding i kildesystemene gjøres i kapittel 1 i denne veiledningen.

3.2 KRAV TIL BRUKER-ADMINISTRATIVT SYSTEM (BAS)

Et brukeradministrativt system mottar informasjon fra autoritative datakilder og håndterer denne. Feide sier at organisasjonen skal ha et slikt brukeradministrativt system:

Krav 3.5: *[Vertsorganisasjonen må] installere et BAS og en LDAP-katalog som kan levere informasjon om brukere til Feide i henhold til de kravene som stilles av Feide [VED1-1, kap. 6].*

Deler av informasjonen som ligger i det brukeradministrative systemet, skal også ligge på vertsorganisasjonens lokale autentiseringstjener, som Feides sentrale innloggingstjeneste har tilgang til.

Vi anbefaler at følgende oppgaver løses med et brukeradministrativt system:

- Generering av passord i henhold til gitte kriterier for sikre passord.
- Sikring av at alle brukernavn er unike, og at de følger navneregler som vil være uforandret over en viss tid.

Vedlegg 2 i denne veiledningen er en sjekkliste for bl.a. brukeradministrative systemer. Før en organisasjon godkjennes som Feide-vertsorganisasjon, vil denne sjekklista bli gjennomgått.

Les mer om brukernavn og passord i temaheftet «Brukernavn og passord - beste praksis».

3.3 KRAV TIL AUTENTISERINGS-TJENER (AT)

Feide må ha tilgang til en viss informasjonsmengde om samtlige Feide-brukere. Dette skjer ved at hver vertsorganisasjon legger ut en såkalt autentiseringstjener, som inneholder et standardsett av opplysninger om organisasjonens brukere. Opplysningene i autentiseringstjeneren hentes automatisk fra det brukeradministrative systemet, og utgjør et subsett av dataene som ligger i det brukeradministrative systemet.

Informasjonens semantikk og struktur er spesifisert i Feides norEdu*-skjema, en nordisk tilpasning av de internasjonale standardskjemaene eduPerson og eduOrg. Organisasjonen har selv ansvar for å administrere og forvalte autentiseringstjeneren:

Krav 3.6: *Organisasjonen skal anvende en autentiseringstjener som er tilpasset Feides arkitektur [KON2, kap. 1.1].*

Brukerdata som ligger i autentiseringstjeneren, skal oppdateres og konsistenssjekkes daglig av organisasjonen. Organisasjonen er ansvarlig for å holde brukerdata oppdatert og må ha klare rutiner for oppdatering. Rutinene må omfatte fjerning av brukere som organisasjonen ikke lenger ønsker å ta ansvar for. Se kapittel 1 for mer informasjon om behandling av personopplysninger.

Autentiseringstjeneren er en LDAP-katalog med norEdu*-spesifikasjonen lagt på. I denne spesifikasjonen er det en del obligatoriske attributter, men også mange valgfrie attributter:

Krav 3.7: *Autentiseringstjeneren skal anvende Feides LDAP-skjema, slik at alle obligatoriske attributter må anvendes og valgfrie attributter kan anvendes. Feides skjema er definert i Feide-kontraktens vedlegg 1–3 [KON2, kap. 1.1].*

norEdu*-spesifikasjonen springer ut fra et felles nordisk samarbeid. Nasjonal lovgivning, etablerte konvensjoner og enkelte andre omstendigheter varierer likevel mellom landene, og i tillegg varierer behovene med tanke på skoleslag, også innad i nasjonene. Noen attributter som er obligatoriske på universitets- og høgskolenivå, kan dermed være irrelevante i grunnopplæringen. Av denne grunn har Feide valgt fra og med versjon 1.5 av spesifikasjonen å skille mellom grunnopplæringen og universitet- og høgskolesektoren når det gjelder obligatoriske krav til attributter.

På grunn av dette er ingen attributter i norEdu*-spesifikasjonen et krav ut fra skjemadefinisjonen. En gitt føderasjon, som Feide, kan erklære enkelte attributter obligatoriske innen denne føderasjonen. Flere av attributtene som er frivillige i norEdu*-spesifikasjonen, er derfor satt som obligatoriske for Feide. Dokumentet «Feides informasjonsmodell for grunnopplæringa» beskriver de attributtene som alltid må være definert. For brukere som skal autentiseres via Feide og for organisasjonen disse brukerne tilhører, må Feides obligatoriske attributter alltid være satt.

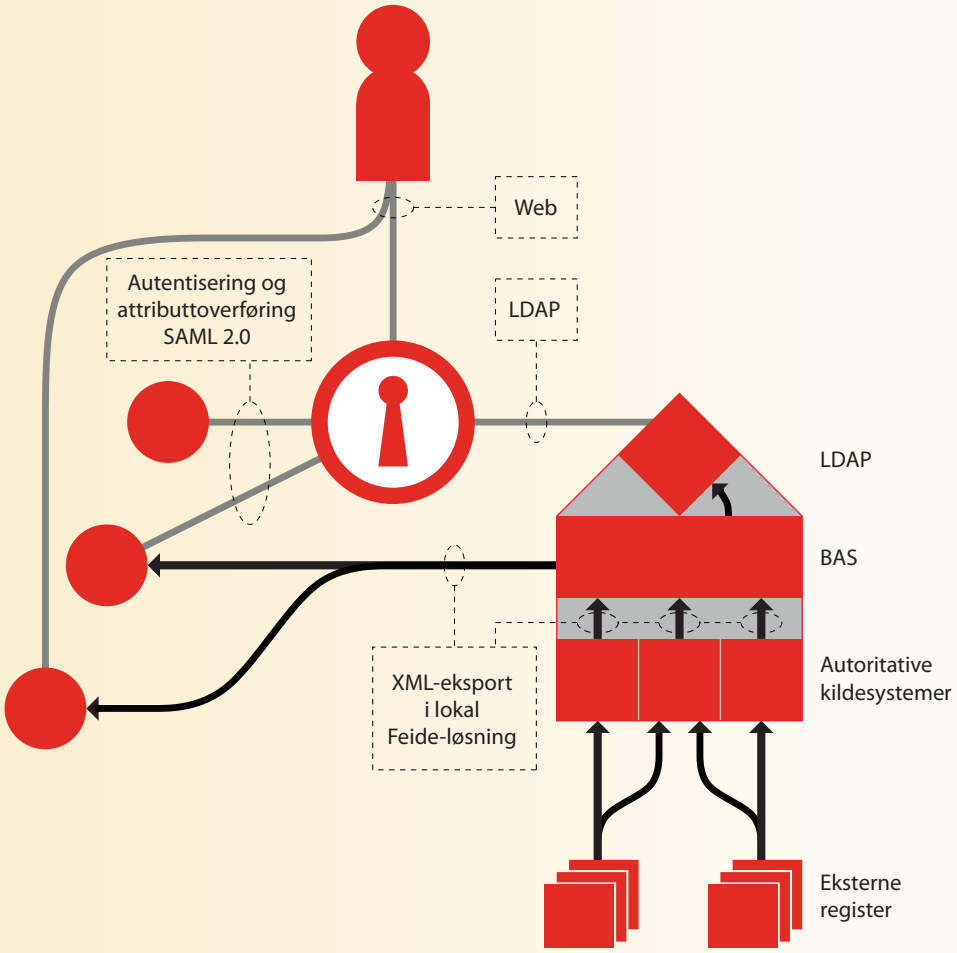
Feide formidler informasjon om Feide-brukere til tjenesteleverandører, og må derfor vite hvilken informasjon de ulike organisasjonene har liggende ute i sine kataloger:

Krav 3.8: *Organisasjonen skal gi Feide informasjon om hvilke av de valgfrie attributtene fra Feides LDAP-skjema som anvendes [KON2, kap. 1.2].*

Dette gjøres ved å benytte kontaktpunkter som definert i kontaktpersoner for vertsorganisasjoner.

For å sikre at informasjonen som ligger i organisasjonens autentiseringstjener er ordnet, oppdatert og korrekt, krever Feide at organisasjonen har et system for identitetsforvaltning:

Krav 3.9: *Informasjonen i katalogen fylles inn fra et system for identitetsforvaltning (et brukeradministrativt system) hos organisasjonen [VED1-1, kap. 3].*


Web
Autentisering og
attributtoverføring
SAML 2.0
LDAP
LDAP
BAS
Autoritative
kildesystemer
XML-eksport
i lokal
Feide-løsning
Eksterne
register

En viktig komponent i et slikt system er det brukeradministrative systemet (BAS). Et brukeradministrativt system henter informasjon om brukere i vertsorganisasjonen fra autoritative kildesystemer, og håndterer denne informasjonen.

Videre må det finnes koblinger eller grensesnitt som gjør at data overføres mellom de autoritative kildesystemene og det brukeradministrative systemet, og mellom det brukeradministrative systemet og autentiseringstjeneren:

Krav 3.10: *Det må være etablert kanaler slik at data automatisk og feilfritt kan flyte fra kildesystemene til LDAP-katalogens grensesnitt mot Feides innloggingstjeneste [VED1-1, kap. 6].*

De automatiske prosedyrene som overfører data fra kildesystemene til autentiseringstjeneren, skal kjøres minst én gang i døgnet for å holde katalogen så oppdatert som mulig. Feide autentiserer brukere via den enkelte brukers vertsorganisasjon, og må ha tilgang til organisasjonens lokale LDAP-katalog:

Krav 3.11: *Organisasjonen skal gi Feide tilgang til oppslag i organisasjonens lokale autentiseringstjener. Teknisk informasjon om lokal autentiseringstjener og kontaktperson for denne skal holdes oppdatert av organisasjonen [KON2, kap. 1.5].*

Feide har tillit til at vertsorganisasjonen korrekt kan bekrefte eller avkrefte om dens brukere oppgir riktig passord. På forespørsel skal også vertsorganisasjonen levere brukerattributter som spesifisert i avtale. Videre plikter vertsorganisasjonen å avvise autentisering av brukere som ikke lenger har tilknytning til organisasjonen.

For at kommunikasjonen mellom organisasjonen og Feides innloggingstjeneste skal fungere, må Feide ha tilgang til autentiseringstjeneren også rent nettverks- og aksessmessig:

Krav 3.12: *Innloggingstjenesten må kjenne til startpunktets DN («Distinguished Name») for Feide-delen av katalogtreet, og må ha rettighet til å søke opp en brukers DN ut fra vedkommendes Feide-navn [VED1-1, kap. 3].*

For teknisk informasjon om hvordan en LDAP-tjener skal settes opp for Feide, se LDAP-skjema for Feide (http://www.feide.no/ldap-schema-feide).

I grensesnittet mellom Feide og den enkelte autentiseringstjener skal det kunne overføres personopplysninger. Denne kanalen må derfor sikres:

Krav 3.13: *Kommunikasjonen mellom autentiseringstjener og Feide skal være pålitelig og sikret mot avlytting [VED1-1, kap. 3].*

Kommunikasjonen mellom autentiseringstjener og Feide sikres med bruk av LDAP og SSL/TLS.

KAP. 4

Krav om førstelinjesupport

UNINETT yter andrelinjesupport overfor vertsorganisasjoner og tjenesteleverandører, men organisasjonene må selv håndtere brukerstøtte overfor sine brukere:

Krav 4.1: *Organisasjonen skal yte førstelinjesupport for egne brukere i tilfelle påloggingsproblemer og andre problemer relatert til Feide [KON2, kap. 3.1].*

Det er viktig at personer i organisasjonen som yter slik brukerstøtte, har fått god opplæring i Feide:

Krav 4.2: *Organisasjonen skal sørge for at alle som jobber med førstelinjesupport har fått adekvat opplæring i Feide [KON2, kap. 3.1].*

SØKNADSPROSESS

DEL

III

KAP. 5

Søknadsprosess for å bli Feide-godkjent

5.1 PROSESS FOR Å BLI VERTSORGANISASJON

En Feide-vertsorganisasjon er en skoleeier som tildeler Feide-navn til sine tilknyttede personer og som håndterer autentiseringsinformasjon og brukerattributter. Vertsorganisasjonen forplikter seg til å følge retningslinjer spesifisert i kontrakten med Feide. Den har lokal identitetsforvaltning på plass, og lar Feides sentrale innloggingstjeneste utføre autentisering av brukere via den lokale løsningen. En organisasjon som oppfyller Feide-kravene, kan søke om å bli Feide-vertsorganisasjon:

Søknadsprosessen foregår i følgende trinn:

(1) Fyll ut søknadsskjema for vertsorganisasjoner. Les mer om berettigetrollen nedenfor.
(2) Etter at søknaden er mottatt, vil organisasjonen bli bedt om å fylle ut en BAS-sjekkliste (se vedlegg 2). Lista inneholder primært spørsmål om rutiner for personopplysninger, men også spørsmål om forankring og kildesystemer m.m. Dersom man har dokumentasjon som dekker hele eller deler av det som etterspørres i sjekklista, kan dette leveres i stedet.
(3) Etter at BAS-lista er levert og eventuelle uklare forhold er avklart, vil kontraktspapirer bli sendt for undertegning (se del 1 og 2 i kontrakten).
(4) Kontrakten signeres og returneres til Feide.
(5) Feide kontrasignerer og returnerer ett eksemplar av kontrakten. Begge parter har da en signert versjon, og avtalen er inngått.

5.1.1 Om rollen berettiget

Berettigede i Feide har en sentral rolle på vegne av sin vertsorganisasjon. Det er disse personene som administrerer hvilke tjenester organisasjonen skal ha tilgang til gjennom Feide. Berettigede får også tilgang til nyttige verktøy for å holde orden på det tekniske rundt Feide. Tenk derfor nøye gjennom hvem som skal være berettiget, og vær sikker på at disse personene er klar over hvilket ansvar det innebærer.

Berettiget er man på vegne av skoleeier. For grunnskolen og videregående opplæring betyr dette at man ikke kan abonnere på tjenester for enkeltskoler, men for alle skoler i kommunen eller fylkeskommunen. En berettiget må eksistere som bruker i vertsorganisasjonens Feide-katalog.

Administrasjon av hvilke tjenester man ønsker tilgang til, gjøres i Feides kundeportal. Der kan man også endre hvem som skal være berettiget. Sørg for at detaljene om hvem som er berettiget, til enhver tid er oppdatert.

Les mer på http://www.feide.no/berettigede.

5.1.2 Om kommunesamarbeid

Mange kommuner går sammen om innføringen av Feide. I Feide er det skoleeier som blir vertsorganisasjon og kontraktspartner. Dette betyr at det må sendes inn separate søknader for hver enkelt kommune i samarbeidet, med opplysninger om egne berettigede. Det er ikke noe i veien for at én enkelt person i kommunesamarbeidet er kontaktperson.

Berettigede bør være en representant for den enkelte skoleeier. Ønsker kommunesamarbeidet likevel at en representant for kommunesamarbeidet skal være berettiget, må denne personen ha egen Feide-bruker for alle de aktuelle kommunene.

5.2 PROSESS FOR Å BLI FEIDE-TJENESTELEVERANDØR

5.2.1 Vertsorganisasjoner som tjenesteleverandør

En Feide-tjeneste er en tjeneste som benytter Feide-innlogging for autentisering av brukere, og som har en avtale med Feide om hvilke brukerattributter som skal hentes. En organisasjon som leverer Feide-tjenester, kalles en Feide-tjenesteleverandør. Vertsorganisasjoner i Feide er gjerne også tjenesteleverandører fordi de leverer tjenester til sine egne brukere. Dette kaller vi gjerne lokale tjenester.

Vertsorganisasjoner i Feide som også ønsker å levere tjenester, trenger ikke å søke om å være tjenesteleverandør. Dette er allerede dekket av kontrakten man har signert som vertsorganisasjon. Tjenesteskjema må imidlertid fylles ut, men da gjennom Feides kundeportal.

5.2.2 Andre tjenesteleverandører

Mange offentlige og kommersielle aktører leverer tjenester til utdanningssektoren, og disse kan søke om å bli Feide-tjenesteleverandør.

Krav 5.1: *For å kunne tilby tjenester med Feide-innlogging, må organisasjonen sende en søknad til Feide om å få bli en tjenesteleverandør [VED1-1, kap. 8.1].*

Det må inngås en kontrakt med Feide. Dette foregår i følgende trinn:

(1) Sende inn søknadsskjema.

(2) Motta kontraktspapirer for signering. Feide gjør en vurdering av om tjenesten er ønskelig å tilby gjennom Feide, og sender deretter ut kontraktspapirer for signering. Disse papirene må signeres og returneres.

(3) Før en tjeneste settes i produksjon, vil Feide i tillegg be om utfylling av et tjenesteskjema. Her spesifiseres flere detaljer for tjenesten, som attributter, URL, teknisk kontakt, beskrivelse etc. Feide trenger også en logo for tjenesten på hvit eller transparent bakgrunn. Logoen vises når man ønsker å logge på tjenesten via Feide.

Dersom en tjenesteleverandør har flere tjenester som skal tilbys gjennom Feide, behøves ingen ny søknad eller ny kontrakt. Dette reguleres gjennom tjenesteskjema som må fylles ut for hver tjeneste.

VEDLEGG
DEL
IV

VEDLEGG 1
Ordliste

Her finner du forklaring på en del begreper du møter i Feide-sammenheng.

BEGREP	DEFINISJON
Autentiseringstjener (AT)	Den lokale autentiseringstjenesten ved en Feide-organisasjon som kan autentisere Feide-navn organisasjonen har tildelt. Teknisk sett er dette en LDAP-tjener som bruker Feide-skjema.
Autoritativ	Det verdialternativ som er definert som korrekt dersom det oppstår konflikt mellom ulike kildesystemer. I Feide skal det for hvert attributt som er tilknyttet en brukertype, identifiseres hvilket kildesystem som er autoritativt, og det må sørges for at dette systemet til en hver tid leverer en korrekt og oppdatert attributtverdi.
Brukeradministrativt system (BAS)	BAS er et informasjonsnav som mottar informasjon fra kildesystemer, behandler denne og sender den ut til mottakersystemer. BAS inneholder og synkroniserer informasjon om brukerne ved en organisasjon, basert på opplysninger fra kildesystemer. BASet oppretter brukere, lager brukernavn og passord og lagrer andre påkrevde opplysninger. I tillegg gir det etter avtale nødvendige opplysninger til tjenester som har behov for informasjon om brukerne.
Feide	Står for Felles Elektronisk IDEntitet. Feide er en enhetlig identitetsforvaltning for utdanningssektoren.
Feide-bruker	En person som har fått tildelt et Feide-navn for pålogging til tjenester.
Feide-innlogging	Bruk av et Feide-navn i Feides felles innloggingstjeneste for å få tilgang til tjenester.
Feide-navn	Et brukernavn tildelt en person av en Feide-organisasjon, inneholder både lokalt brukernavn og organisasjonsinformasjon.
Feide-organisasjon	En organisasjon som har inngått avtale med UNINETT om bruk av Feide.

Identitetsforvaltning	Identitetsforvaltning handler om å identifisere individer og kontrollere deres tilgang til ulike ressurser. Altså: Hvem er du og hva har du lov til? Elektronisk identitetsforvaltning handler om at individer kan identifisere seg elektronisk og få tilgang til digitale ressurser eller tjenester.
Kildesystemer	Vertsorganisasjoner må ha en lokal Feide-løsning, dvs. brukeradministrativt system og autentiseringstjener. Dataene som brukes av den lokale Feide-løsningen vedlikeholdes ikke der, men i kildesystemer. Kildesystemer er IT-systemer som i tillegg til å ha sin egen funksjonalitet, f.eks. for administrasjon av et lærested, også fungerer som datakilde for den lokale Feide-løsningen.
LDAP	En database som er strukturert på en bestemt måte (kalles elektronisk katalog). Man kommuniserer med databasen ved hjelp av en standard kalt LDAP (Lightweight Directory Access Protocol). Katalogen inneholder som regel informasjon om personer og institusjoner.
Moria	Feides innloggingstjeneste.
norEdu*	Feides LDAP-skjema for informasjon om personer og organisasjoner i utdanningssektoren. norEdu* er basert på de internasjonale definisjonene eduOrg og eduPerson utviklet i regi av EDUCAUSE. norEdu* er utviklet i nordisk regi, under ledelse av Feide.
Rolle	Roller er Feides generelle grupperingsmekanisme. Feide opererer med et sett av roller, ansatt og elev er to eksempler. Feides rollesett er i utgangspunktet definert av et internasjonalt samarbeid.
SSL	Forkortelse for Secure Socket Layer. En nettverksprotokoll som brukes for å sette opp krypterte forbindelser. Brukes for eksempel av mange websider der kredittkortinformasjon og lignende innhentes. En webadresse som krever SSL starter med https i stedet for http.
Tjenesteleverandør	En Feide-tjenesteleverandør er en organisasjon som yter tjenester til personer i utdanningssektoren, og benytter Feide-innlogging til å autentisere dem.
TLS	Forkortelse for Transport Layer Security. Etterfølgeren til SSL (se denne) med samme bruksområde.
Vertsorganisasjon	En Feide-vertsorganisasjon er en skoleeier som gir Feide-navn til sine elever, studenter, ansatte og andre tilknyttede personer. Vertsorganisasjonen henter data fra personopplysningene i vertsorganisasjonens elev-, student- og personalregistre. Vertsorganisasjoner i Feide er ofte også Feide-tjenesteleverandører.

VEDLEGG 2

Sjekkliste for BAS

INNFØRING AV FEIDE

- Hvordan har forankringen av Feide foregått i ledelsen?
- I hvilke(t) besluttende fora har Feide vært behandlet, og hvilke formelle beslutninger er tatt?

PERSONDATA GENERELT

- Er ansvaret for kvaliteten på persondataene klart og entydig plassert?
- Er det etablert systematisk samarbeid med faste gjennomganger mellom avdelinger med hensyn til persondata?

SKRIFTLIGE RUTINER

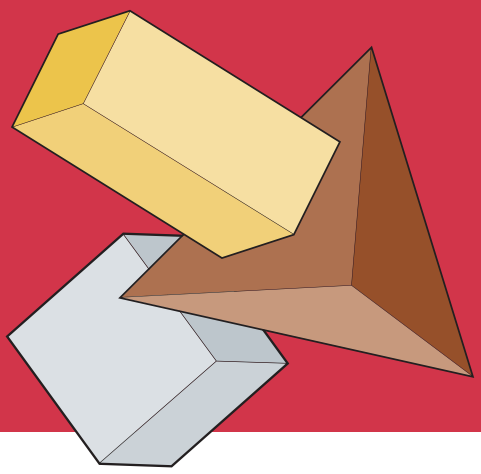
- Legg ved de skriftlige rutiner som måtte finnes for håndtering av nye brukere, brukere som slutter samt vedlikehold av brukerdata for elever, studenter, ansatte og ev. andre roller.
- Hvis de ikke finnes skriftlig, beskriv rutinene med egne ord. Få spesielt med hvordan elever/studenter som har sluttet/ikke lenger er oppmeldt i noen fag, samt hvordan ansatte som har sluttet, håndteres.
- Hvordan sikrer man at disse rutinene følges?
- Hvordan vil slike endringer gjenspeiles i Feide-katalogen?
- Har det blitt nødvendig med innlegging eller endring av data direkte i BAS, i tilfelle hvilke tilfeller og hvordan er rutinene rundt denne håndteringen dokumentert?
- Hvordan kobles personer i/til hhv. organisasjoner og roller?
- Kilder for ulike roller; ansatte/elev/student/andre
- Hvilke roller opereres det med, og hva er kriteriene for å bli tildelt de ulike rollene?
- Hva er kildene for ansattedata, elev-/studentdata og ev. andre roller per i dag?
- Hvor ofte legges det inn data i disse respektive kildene, og hvor ofte eksporteres data ut fra disse kildene?

BRUKERKONTO

- Hvilke krav stilles til brukerenes passord?

BAS-LØSNING

- Er det etablert samarbeid med andre institusjoner med lignende løsninger for BAS?
- Fungerer samarbeidet med ev. ekstern leverandør av BAS godt?



SENTER
FOR IKT I
UTDANNINGEN

www.iktsenteret.no