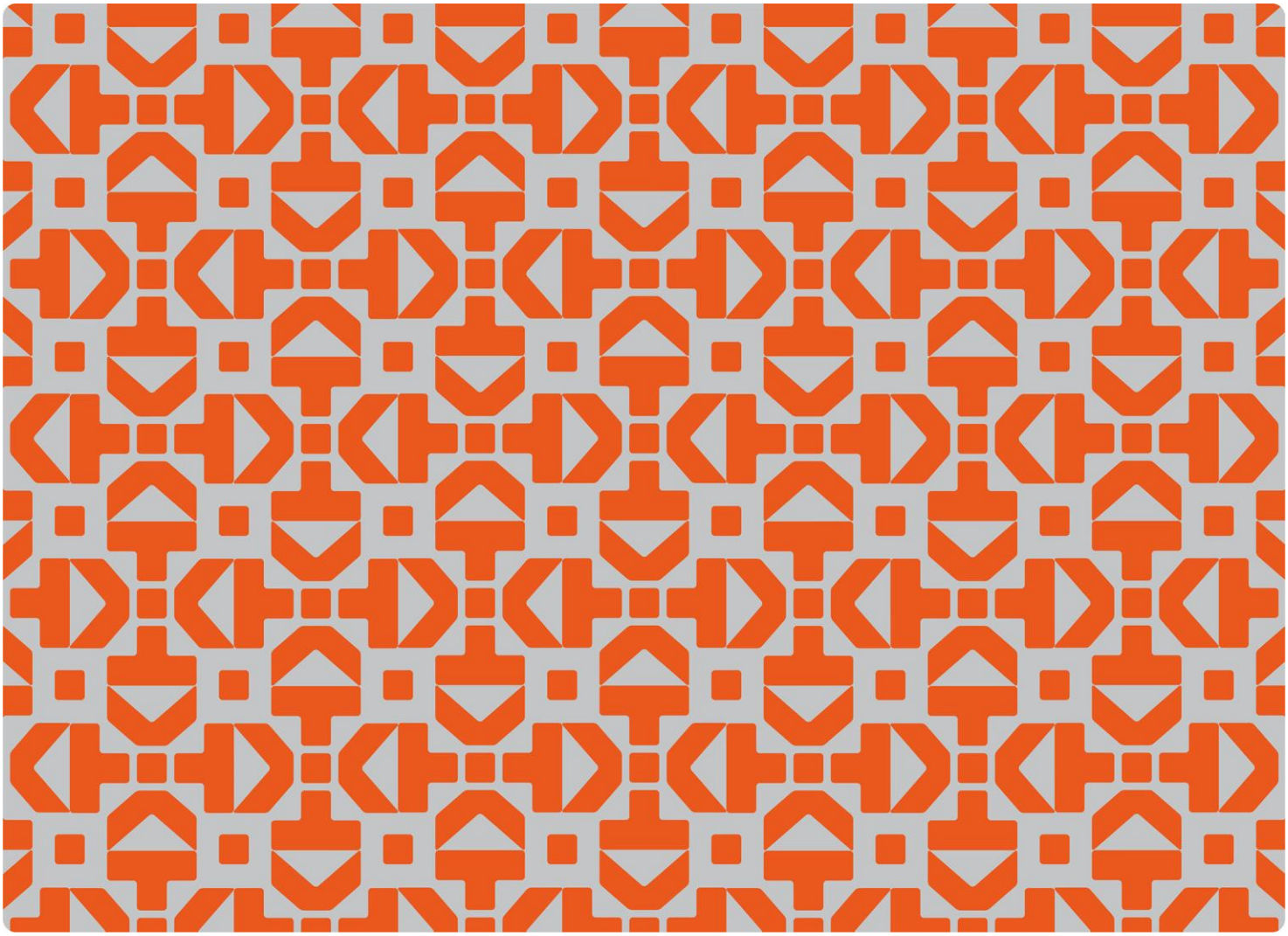
Direktoratet for høyere utdanning og kompetanse

Rapport nr. 17/2022

Praktisering av krav til informasjonssikkerhet og personvern

Samsvar og avvik hos statlige universiteter og høgskoler



Praktisering av krav til informasjonssikkerhet og personvern

Samsvar og avvik hos statlige universiteter og høgskoler

Redaktør:
Ragnhild Tungesvik

Forfattere:
Tommy Tranvik
Benjamin Gangvik

ISSN 2703-9102
Utgitt: 11/2022

Innhold

Sammendrag

Kunnskapsdepartementets policy for informasjonssikkerhet og personvern tydeliggjør hvilke krav som stilles til dette arbeidet hos de 28 statlige universitetene og høgskolene, øvrige forvaltningsorganer og selskaper som omfattes av departementets policy. Hvert år kartlegger og vurderer HK-dir etterlevelsene av kravene i policyen hos disse institusjonene og virksomhetene.

I denne temarapporten presenteres den mest typiske – eller vanlige – formen for etterlevelse av 13 viktige krav i policyen. Dette gjøres for de 21 statlige universitetene og høgskolene, men ikke for de øvrige sju forvaltningsorganene og selskapene.

Den typiske etterlevelsen av hvert enkelt av de 13 kravene defineres av det vi omtaler som median-institusjonen. Medianen er den formen for etterlevelse vi finner hos institusjonen i midten av utvalget på 21 universiteter og høgskoler når disse sorteres etter graden av etterlevelse (fra høyest til lavest).

Institusjoner og virksomheter i UH-sektoren kan benytte rapporten til å vurdere hva som er bra og mindre bra «hos oss» sett opp mot «det typiske». Det kan være nyttig i det videre arbeidet med å styrke policyetterlevelsen.

De viktigste funnene

Median-institusjonen overholder i hovedsak følgende av de 13 kravene som behandles i denne rapporten:

- toppledelsens og styrets involvering i arbeidet med informasjonssikkerhet og personvern (men med enkelte forbehold),
- etablering av rutiner for ivaretakelse av de registrertes personvernrettigheter,
- utnevning av personvernombud (men med enkelte forbehold),
- generell bevisstgjøring av studenter og ansatte med hensyn til informasjonssikkerhet og personvern.

Det kan ikke påvises avvik hos median-institusjonen for to av de andre kravene i policyen som drøftes i rapporten. Dette gjelder forhold hvor den enkelte institusjon selv må vurdere om tilstanden er tilfredsstillende eller ikke:

- Om antall og typer uønskede hendelser og brudd på informasjonssikkerheten indikerer at det er behov for å styrke sikkerhetsarbeidet. Det kan likevel være behov for å styrke evnen til å oppdage brudd og utbedre sårbarheter.

- Om ressursinnsatsen – antall årsverk øremerket til arbeidet med informasjonssikkerhet og personvern – bør styrkes. Andre avvik kan indikere at ressursinnsatsen likevel bør prioriteres sterkere.

Til slutt viser rapporten at median-institusjonen har enkelte avvik fra flere av de øvrige kravene som drøftes:

- iverksetting (praktisering) av ledelsessystem for informasjonssikkerhet i alle deler av kjernevirksomheten,
- etablere en fungerende sikkerhetsorganisering i alle deler av kjernevirksomheten,
- gjennomføring av risikovurderinger og oppfølging av vurderingene med nødvendige sikringstiltak,
- oppfølging av og kontroll med behandlinger av personopplysninger som er tjenesteutsatt (bruk av databehandlere),
- overføringer av personopplysninger til tredjeland,
- utarbeidelse av fullstendige planer for håndtering av alvorlige digitale sikkerhetshendelser og opprettholdelse av kritiske funksjoner/oppgaver (beredskap og kontinuitet),
- iverksetting (praktisering) av internkontroll for personvern (GDPR) i alle deler av kjernevirksomheten,
- utarbeidelse av en fullstendig protokoll for behandling av personopplysninger (behandlingsprotokoll),
- rollespesifikk opplæring av ledere og medarbeidere som er ment å utføre viktige informasjonssikkerhets- eller personvernoppgaver.

Datagrunnlaget

Datagrunnlaget for rapporten er HK-dir sin kartlegging av universitetenes og høgskolenes praktisering av departementets policy i 2021 og 2022.

Innledning

I november 2021 til februar 2022 gjennomførte HK-dir sin fjerde årlige kartlegging av informasjonssikkerhet og personvern i UH-sektoren.[1] De årlige kartleggingene har blant annet til hensikt å vurdere hvordan 28 statlige universiteter, høgskoler, øvrige forvaltningsorganer og selskaper[2] etterlever kravene i «Kunnskapsdepartementets policy for informasjonssikkerhet og personvern i høyere utdanning og forskning».[3]

På bakgrunn av kartleggingene, publiserer HK-dir årlige risiko- og tilstandsvurderinger. Denne temarapporten supplerer risiko- og tilstandsvurderingene ved å beskrive hva som er den typiske (mest vanlige) praktiseringen av viktige krav i departementets policy. Dette gjøres for de 21 statlige universitetene og høgskolene.

Den typiske etterlevelsen hos de resterende sju forvaltningsorganene og selskapene som også omfattes av departementets policy, drøftes ikke. En slik beskrivelse vil bli publisert etter kartleggingen i 2022-2023.

Kartlegginger, sektorstyring og policy
Resultatene fra de årlige kartleggingene danner grunnlag for departementets og HK-dir sin styring av arbeidet med informasjonssikkerhet og personvern i UH-sektoren. Det betyr at departementet og HK-dir følger opp resultatene fra kartleggingene overfor den enkelte institusjon og virksomhet.

Hvordan sektorstyringen for øvrig foregår – og oppgavefordelingen mellom departementet og HK-dir – beskrives nærmere i Kunnskapsdepartementets styringsmodell for informasjonssikkerhet og personvern.[4] Departementet har det overordnede ansvaret for informasjonssikkerhet og personvern i UH-sektoren. HK-dir har ansvaret for den løpende sektorstyringen.

[1] Resultatene fra kartleggingene oppsummeres og drøftes i årlige tilstands- og risikovurderinger. Disse er tilgjengelige på https://www.unit.no/styring-av-informasjonssikkerhet-og-personvern-i-hoyere-utdanning-og-forskning. Sist besøkt 1.11.2022.

[2] Vedlegg 1 gir en oversikt over de 28 institusjonene og virksomhetene som omfattes av Kunnskapsdepartementets policy.

[3] Departementets policy er tilgjengelig på https://www.regjeringen.no/no/dokumenter/f-04-20-policy-for-informasjonssikkerhet-og-personvern-i-hoyere-utdanning-og-forskning/id2769629/. Sist besøkt 1.11.2022.

[4] Nærmere beskrivelser av styringsmodellen er tilgjengelig på https://www.unit.no/styring-av-informasjonssikkerhet-og-personvern-i-hoyere-utdanning-og-forskning. Sist besøkt 1.11.2022.

Policyen for informasjonssikkerhet og personvern er en del av Kunnskapsdepartementets styringsmodell. Policyen oppsummerer gjeldende rettslige krav for arbeidet med informasjonssikkerhet og personvern. Den inneholder derfor ingen krav ut over det som allerede er lovpålagt.

Kort oppsummert innebærer policyen at (i) arbeidet med informasjonssikkerhet skal være risikobasert og skje innenfor rammen av et ledelsessystem, og (ii) det skal etableres og vedlikeholdes en internkontroll for behandling av personopplysninger som sørger for lovlig og forsvarlig håndtering av opplysningene.

Fremgangsmåten – hvordan finne det typiske?

For å avgjøre hva som er den mest typiske formen for etterlevelse, har vi har tatt utgangspunkt i 13 viktige krav i departementets policy for informasjonssikkerhet og personvern. Dette er krav som HK-dir hvert år kartlegger institusjonenes praktisering av.

Deretter har vi sortert utvalget – de 21 statlige universitetene og høgskolene – i henhold til graden av etterlevelse (fra høyest til lavest). Dette er gjort for hver enkelt av kravene som behandles i denne rapporten.

Når utvalget (institusjonene) er sortert, har vi forsøkt å finne medianen. Medianen er den praktisering av krav vi finner hos institusjonen i midten, det vil si den som deler utvalget i to like store deler når de 21 universitetene og høgskolene er sortert etter graden av etterlevelse – institusjon nummer 11. Vi omtaler denne institusjonen som median-institusjonen. Det betyr at 10 institusjoner har høyere grad av policyetterlevelse enn median-institusjonen. De 10 andre institusjonene har noe lavere grad av etterlevelse.

I denne temarapporten er det altså etterlevelsen hos median-institusjonen – institusjon nummer 11 – som beskriver hva som er den mest typiske (vanlige) praktiseringen av hver enkelt av de 13 kravene.

Samling i midten

Mange av de 21 statlige universitetene og høgskolene befinner seg på omtrent samme nivå når det gjelder praktisering av kravene i policyen. Tendensen til «samling i midten» – relativt små variasjoner i policyetterlevelsen mellom mange av institusjonene – gjør at beskrivelsene av «det typiske» (medianen) er gyldig for en stor del av utvalget. Vi mener derfor at mediainstitusjonen viser et overordnet bilde av hva som er tilstanden hos mange av institusjonene.

For enkelte institusjoner er imidlertid beskrivelsene av «det typiske» mindre dekkende. Det gjelder primært for institusjoner som har kommet langt i sitt arbeid med etterlevelse av policykravene.

Medianen er ikke målet
Det er ikke meningen at praktiseringen av policyen hos median-institusjonen skal benyttes som standard for hva institusjoner og virksomheter som omfattes av policyen skal oppnå, for eksempel at «hos oss er vi fornøyd med å være der hvor mange andre i sektoren befinner seg.»

Hva som skal oppnås følger utelukkende av «Kunnskapsdepartementets policy for informasjonssikkerhet og personvern i høyere utdanning og forskning».

Institusjoner og virksomheter i UH-sektoren kan likevel anvende medianen (og median-institusjonen) til å vurdere eget ståsted – hva som er bra og mindre bra «hos oss» sett opp mot «det typiske» – og hva det kan innebære av forbedringer for å styrke policyetterlevelsen.

Rapporten kan også gi nyttig informasjon til institusjoner eller virksomheter som ønsker å tilby tjenester til sektoren som bidrar til lukking av avvik og forbedring av tilstanden.

Sektorprofilen
Når vi ser den typiske (vanlige) praktiseringen av policykravene under ett, utgjør dette en profil for arbeidet med informasjonssikkerhet og personvern hos de statlige universitetene og høgskolene – en sektorprofil.

Sektorprofilen gir nøkkelinformasjon om hva som særpreger dette arbeidet hos institusjonene.

Vi oppsummerer sektorprofilen i siste del av rapporten.

Median-institusjonen – krav, praktisering og samsvar

I det følgende gjør vi rede for hvordan median-institusjonen praktiserer hvert av de 13 kravene i Kunnskapsdepartementets policy for informasjonssikkerhet og personvern.

Redegjørelsen har følgende oppbygning:

- Først viser vi til hvilke punkter i policyen som det enkelte krav følger av.
- Deretter beskrives (kort) median-institusjonens praktisering av det enkelte krav.
- Til slutt angir vi hvordan praksis hos median-institusjonen samsvarer med eller avviker fra det som policyen krever.

Informasjonssikkerhetshendelser	
Krav i policyen	Punkt 1 og 1b i departementets policy stiller krav om at informasjonssikkerheten er tilfredsstillende. I punkt 6 stilles det krav til etablering av prosesser og rutiner for riktig og lovlig håndtering av personopplysninger. Dette inkluderer forsvarlig sikring av personopplysninger som institusjonene behandler. Policyen inneholder ikke mål for antallet uønskede hendelser, verken på sektor- eller institusjonsnivå. Institusjonene må selv vurdere om de brudd på informasjonssikkerheten som registreres er i tråd med det som er definert som akseptabelt (risikoaksept). Det er et lederansvar å bestemme institusjonens risikoaksept, jf. punkt 1b.
Praktisering av kravene	Median-institusjonen rapporterer om 17-20 kjente informasjonssikkerhetshendelser og -avvik i året (2021).[5] Dette inkluderer hendelser som gjelder sikkerheten til personopplysninger. Nettkriminalitet (økonomisk motiverte forsøk på svindel) er den største kategorien hendelser. Forsøkene lykkes vanligvis ikke.

[5] Rapporterte informasjonssikkerhetshendelser og -avvik er et område hvor det er til dels store variasjoner mellom institusjonene. Mye av variasjonen kan trolig forklares av to forhold. For det første, størrelsen på institusjonenes «digitale fotavtrykk» (spesielt omfanget av datanettverket – antall datamaskiner og brukere – og mangfoldet av dataprogrammer og IT-tjenester som anvendes). For det andre, evnen til å oppdage uønskede hendelser og avvik, inkludert forskjeller i bruken av tekniske deteksjonssystemer.

	Deretter følger uønskede hendelser som skyldes menneskelige eller tekniske feil og uhell. Typiske eksempler på menneskelig feil/uhell er feilsending av eposter, lagring av personopplysninger hvor de er tilgjengelig for uvedkommende og feilpublisering av slike opplysninger på internett. I 2021 registrerte median-institusjonen minst ett tilfelle hvor det er mistanke om forsøk på statlig hacking.
Samsvar og avvik	Det påvises ikke avvik fra informasjonssikkerhetskravene i policyen nevnt ovenfor. Institusjonen må selv avgjøre om antall og typer uønskede hendelser er i henhold til egen risikoaksept, og iverksette nødvendige forbedringstiltak dersom det ikke er tilfelle. Det er likevel trolig at evnen til raskt å oppdage sikkerhetsbrudd og avvik – og utbedre sårbarheter – bør styrkes. På bakgrunn av HK-dir sine årlige kartlegginger av arbeidet med informasjonssikkerhet og personvern, mener direktoratet at løsepengevirus, kompromitterte kontoer og statlig hacking er trusler som sektoren bør være særlig oppmerksom på.[6]

Ressurser (årsverk)	
Krav i policyen	Punktene 1d og 4i i departementets policy stiller krav om at arbeidet med informasjonssikkerhet tilføres tilstrekkelige ressurser. Dette er et lederansvar. I policyens punkt 8b understrekes det at også personvernombudet må ha tilstrekkelige ressurser til å ivareta sine oppgaver.
Praktisering av kravene	Median-institusjonen har øremerket totalt fire årsverk til arbeidet med informasjonssikkerhet og personvern. Årsverkstallet inkluderer stillingsprosenten til personvernombudet. Rollen som personvernombud utgjør i gjennomsnitt knapt 60 prosent av et helt årsverk i universitets- og høgskoledelen av sektoren.[7]

[6] Se spesielt «Risiko- og tilstandsvurdering 2022», side 76-79. Rapporten er tilgjengelig på https://hkdir.no/rapportar/informasjonssikkerhet-og-personvern-i-hoeyere-utdanning-og-forskning. Sist besøkt 1.11.2022.

[7] Sju av de 21 universitetene og høgskolene opplyser om at personvernombudet er ansatt i 100 prosent stilling.

	I tillegg til personvernombudet, er årsverkene hos median-institusjonen i stor grad knyttet til IT-avdelinger/seksjoner og andre deler av administrasjonen, inkludert forskningsadministrasjon. Median-institusjonen gir ikke overslag over ressursinnsatsen til de vitenskapelig ansatte når det gjelder informasjonssikkerhet og personvern.
Samsvar og avvik	Det påvises ikke avvik fra kravene i policyen nevnt ovenfor. Det er institusjonens ansvar å vurdere om ressursinnsatsen er tilstrekkelig til å overholde kravene i Kunnskapsdepartementets policy, og å sikre et tilfredsstillende nivå på informasjonssikkerheten. Gjennomgangen av median-institusjonens praktisering av øvrige krav i policyen (se nedenfor) kan likevel indikere at ressursinnsatsen bør styrkes.

Ledelsessystem for informasjonssikkerhet	
Krav i policyen	Punkt 1 i departementets policy stiller krav om at arbeidet med informasjonssikkerhet skal være systematisk og planmessig. Arbeidet skal inngå i den generelle virksomhetsstyringen. Dette er et lederansvar, og skal skje gjennom etablering og iverksetting (praktisering) av et ledelsessystem for informasjonssikkerhet. Ledelsessystemet skal dokumenteres, jf. punkt 12 i policyen. Øvrige krav i punktene 1-5 og 11 i policyen spesifiserer nærmere hvilke oppgaver som inngår i et ledelsessystem for informasjonssikkerhet.
Praktisering av kravene	Median-institusjonen har utarbeidet et dokumentert ledelsessystem for informasjonssikkerhet. Hos median-institusjonen er ledelsessystemet forankret hos toppledelsen og styret. Det er opprettet et koordinerende organ for innføring og videreutvikling av ledelsessystemet (forum/nettverk for informasjonssikkerhet og personvern, se «Organisering av arbeidet» nedenfor). Ledelsessystemet – og oppgavene som inngår i det – er ikke godt nok kjent og mangelfullt iverksatt (praktisert) i deler av organisasjonen. Spesielt på enhetsnivå har median-institusjonen utfordringer med å sørge for at sentrale oppgaver utføres slik som forutsatt.

Samsvar og avvik	Median-institusjonen overholder i noen grad de kravene som policyen stiller til etablering og praktisering av ledelsessystem for informasjonssikkerhet. Manglende innføring (praktisering) av ledelsessystemet i hele organisasjonen (alle deler av kjernevirksomheten) er et avvik fra kravene i departementets policy, jf. spesielt punkt 1a. Særlig på enhetsnivå mangler median-institusjonen noe av den kapasiteten og kompetansen som kreves for å utføre viktige sikkerhetsoppgaver.

Organisering av arbeidet	
Krav i policyen	Punkt 1c i departementets policy krever at organiseringen av arbeidet med informasjonssikkerhet skal defineres og dokumenteres. Sikkerhetsorganiseringen er en viktig del av ledelsessystem for informasjonssikkerhet. Dokumentasjonen beskriver hvem toppledelsen har delegert det daglige ansvaret for informasjonssikkerheten til, og hvem (hvilke roller) som skal utføre de ulike oppgavene som inngår i ledelsessystemet. Punkt 4b og 4c i policyen anbefaler at håndtering av digitale sikkerhetshendelser organiseres særskilt, det vil si gjennom opprettelse av egne hendelseshåndteringsteam (IRT).
Praktisering av kravene	Median-institusjonen har delegert ansvaret for det daglige arbeidet med informasjonssikkerhet til en informasjonssikkerhetsleder (CISO). I samarbeid med personvernombudet, har CISO også ansvar for arbeidet med personvern (GDPR). Hos median-institusjonen bistås CISO (og personvernombudet) av utvalgte ressurspersoner. Disse er organisert i et forum/nettverk for informasjonssikkerhet og personvern. Median-institusjonen har opprettet et eget hendelseshåndteringsteam i IT-avdelingen (IRT).
Samsvar og avvik	Median-institusjonen overholder de kravene som policyen stiller til etablering og dokumentasjon av sikkerhetsorganiseringen. Nedenfor skal vi se at det kan påvises avvik med hensyn til iverksetting av organiseringen (utførelsen av sikkerhetsoppgaver), spesielt på enhetsnivå.

Toppledelsen og styret	
Krav i policyen	Punktene 1 og 6 i departementets policy stiller en rekke krav til toppledelsens og styrets ansvar for, kontroll med og involvering i arbeidet med informasjonssikkerhet og personvern. Her forventes det blant annet at toppledelsen stiller tydelige krav til og følger opp arbeidet med informasjonssikkerhet og personvern. I punktene 1g og 6i stilles det krav om at styret skal kontrollere arbeidet med informasjonssikkerhet og personvern.
Praktisering av kravene	Hos median-institusjonen blir toppledelsen informert om arbeidet med informasjonssikkerhet og personvern. Dette skjer primært gjennom ledelsens gjennomgang. Ledelsens gjennomgang avholdes én gang i året.[8] Ut over dette er toppledelsen relativt lite involvert i arbeidet med informasjonssikkerhet og personvern. Hos median-institusjonen orienteres styret om status og planer for arbeidet med informasjonssikkerhet og personvern. Dette skjer i etterkant av ledelsens gjennomgang. Årlig rapport fra personvernombudet fremlegges for styret (orienteringssak).
Samsvar og avvik	Median-institusjonen overholder i hovedsak de krav som policyen stiller. Det kan likevel tenkes at styret bør styrke sin kontroll av arbeidet med informasjonssikkerhet og personvern, jf. punkt 1g og 6i i policyen.

Risikostyring (vurderinger og tiltak)	
Krav i policyen	Punkt 3 i departementets policy krever at institusjonene forebygger brudd på informasjonssikkerheten. Det skal skje ved at det gjennomføres risikovurderinger av sikkerheten i digitale løsninger, behandlinger av personopplysninger og håndtering av annen viktig informasjon.

[8] Temarapporten «Ledelsens styring og kontroll av arbeidet med informasjonssikkerhet» (2021) gjør rede for hvordan ledelsens gjennomgang gjennomføres og hva som diskuteres på disse møtene. Rapporten gjør også nærmere rede for universitets- og høgskolestyrenes kontroll av arbeidet med informasjonssikkerhet og personvern. Temarapporten er tilgjengelig her: https://hkdir.no/rapportar/temarapport-2021-ledelsens-styring-og-kontroll-av-arbeidet-med-informasjonssikkerhet. Sist besøkt 1.11.2022.

	I punktene 3b og 3c kreves det først at risikovurderinger gjennomføres før digitale løsninger tas i bruk for første gang, og at vurderingene oppdateres ved behov. Dernest kreves det at dersom vurderingene viser at risikoen for brudd på informasjonssikkerheten og krenkelser av personvernet er høyere enn hva institusjonen har definert som akseptabelt, skal det iverksettes tiltak for å styrke sikkerheten.
Praktisering av kravene	Median-institusjonen har etablert planer og metodikk for risikostyring av informasjonssikkerhet. Planverket følges opp og metodikken anvendes i deler av organisasjonen, primært i IT-avdelingen/seksjonen. I resten av median-institusjonen er ikke systematikken i risikostyringen på samme nivå som i IT-avdelingen/seksjonen: risikovurderinger gjennomføres mer ad hoc. Det samme gjelder etablering av nødvendige sikringstiltak og revisjon av de risikovurderingene som er gjennomført. Risikostyringen utenfor IT-avdelingen/seksjonen er i stor grad avhengig av støtte, tilrettelegging og oppfølging fra ressurspersoner i sentraladministrasjonen. Median-institusjonen gjennomførte flere viktige sikringstiltak i 2021, for eksempel innføring av totrinnsinnlogging og forbedret tilgangs- og rettighetsstyring.
Samsvar og avvik	Median-institusjonen overholder i noen grad de kravene som policyen stiller til risikostyring av informasjonssikkerhet. Manglende systematikk i risikostyringen utenfor IT-avdelingen/seksjonen, er et avvik fra kravene i policyen nevnt ovenfor, jf. spesielt punkt 3b og 3c. Median-institusjonen har behov for økt risikostyringskompetanse blant ledere og medarbeidere utenfor IT-avdelingen/seksjonen. Kompetansebehovet er særlig knyttet til praktiske forhold ved gjennomføring og oppfølging av risikovurderinger.

Tjenesteutsetting (databehandlere) [9]	
Krav i policyen	Punkt 5 i departementets policy stiller krav om at institusjonene sørger for kontroll med leverandører av digitale tjenester hvor personopplysninger behandles (databehandlere).

[9] Bruk av databehandlere i UH-sektoren drøftes nærmere i temarapporten «Tjenesteutsetting av digitale systemer og tjenester». Rapporten er tilgjengelig på https://www.unit.no/styring-av-informasjonssikkerhet-og-personvern-i-hoyere-utdanning-og-forskning. Sist besøkt 1.11.2022.

	Det innebærer blant annet at institusjonene skal forsikre seg om at leverandøren ivaretar personopplysningssikkerheten på en tilfredsstillende måte, og at øvrige krav til behandling av personopplysninger blir overholdt. Krav til sikkerhet og personvern skal reguleres i en avtale med tjenesteleverandøren (databehandleravtaler). I punktene 5c og 5d kreves det at institusjonen forsikrer seg om at vilkår i databehandleravtaler overholdes av tjenesteleverandøren, og at opplysningene bare overføres til tredjeland (land utenfor EU/EØS) når vilkårene for slike overføringer er oppfylt.
Praktisering av kravene	Median-institusjonen har etablert rutiner for risikovurdering av personopplysningssikkerhet i digitale tjenester levert av eksterne aktører (databehandlere). Median-institusjonen har tilsvarende rutiner for inngåelse av avtaler med leverandører av digitale tjenester (databehandleravtaler). Det savnes rutiner for avtalestyring (oppfølging og kontroll av at vilkår i databehandleravtaler overholdes av tjenesteleverandøren). Median-institusjonen praktiserer rutinene for risikovurderinger og inngåelse av databehandleravtaler når det gjelder utsetting og drift av større digitale tjenester (læringsplattformer, plagiatkontroll, økonomi- og regnskapssystemer, Office 365, osv.). Det er mer usikkert om dette også gjøres ved bruk mindre tjenester på fakultets- eller instituttnivå. Median-institusjonen har vurdert om det overføres personopplysninger til tredjeland, særlig USA. Det er usikkert om vilkårene for overføringer er oppfylt for alle digitale tjenester hvor slike overføringer skjer. Median-institusjonen sørger i liten grad for oppfølging og kontroll av at vilkårene i databehandleravtaler overholdes.
Samsvar og avvik	Median-institusjonen overholder de kravene som gjelder før store og viktige digitale tjenesteleveranser tas i bruk. Det kan være avvik når det gjelder digitale tjenester som tas i bruk på fakultets- eller instituttnivå. Manglende oppfølging av og kontroll med databehandlere er et avvik fra kravene i policyen nevnt ovenfor, jf. punkt 5c. Det samme kan være tilfelle for overføringer av personopplysninger til tredjeland, jf. punkt 5d.

Hendelseshåndtering – beredskap og kontinuitet	
Krav i policyen	Punkt 4 i departementets policy krever at det etableres hensiktsmessige tiltak for å oppdage, varsle og håndtere brudd på informasjonssikkerheten. Det samme gjelder for avvik fra rutiner for behandling av personopplysninger, og varsling til Datatilsynet ved alvorlige brudd på personopplysningssikkerheten. Det anbefales at det opprettes egne team for håndtering av alvorlige digitale sikkerhetsbrudd (IRT), jf. punktene 4b-4d (se «Organisering av arbeidet» ovenfor). I punktene 4e, 4f og 4i stilles det krav til håndtering av sikkerhetsbrudd som innebærer langvarig bortfall av digitale løsninger. Oppgavene som løsningene understøtter må kunne opprettholdes til tross for bortfallet. Tjenestenivået behøver ikke å tilsvare det som er vanlig i en normalsituasjon. Det skal øves på håndtering av alvorlige digitale sikkerhetsbrudd.
Praktisering av kravene	Median-institusjonen har etablert interne rutiner for varsling av brudd på personopplysningssikkerheten. Årlig varsles det om relativt få slike sikkerhetsbrudd, men antallet har økt noe siden 2018.[10] Hendelseshåndteringsteam (IRT) er opprettet for håndtering av digitale sikkerhetshendelser. IRT mottar varsler om hendelser og sårbarheter fra sektorens responsmiljø (SRM). Median-institusjonen har etablert en generell beredskapsplan. Beredskapsplanen omfatter enkelte tiltakskort for håndtering av alvorlige digitale sikkerhetshendelser. Median-institusjonen har utarbeidet katastrofeplaner («disaster recovery») for enkelte av de sentrale tjenestene, men mangler en plan for opprettholdelse av kritiske oppgaver ved langvarig bortfall av digitale tjenester, systemer eller infrastruktur. Median-institusjonen gjennomfører fra tid til annen øvelser på håndtering av alvorlige digitale sikkerhetshendelser. Øvelsene fokuserer særlig på personopplysningssikkerheten.
Samsvar og avvik	Median-institusjonen overholder i noen grad de kravene som policyen stiller til hendelseshåndtering, beredskap og kontinuitet. Manglende tiltakskort for digitale sikkerhetshendelser og planverk for opprettholdelse av kritiske oppgaver ved alvorlige digitale sikkerhetshendelser, er avvik fra kravene i policyen

[10] I gjennomsnitt ble Datatilsynet varslet om drøyt to brudd på personopplysningssikkerheten i 2021 (fra de statlige universitetene og høgskolene). Dette gjennomsnittstallet er noe høyere enn hva det var i de tre foregående årene.

	nevnt ovenfor, jf. spesielt punkt 4e og 4i.

Internkontroll for personvern (GDPR)	
Krav i policyen	Punkt 6 i departementets policy stiller krav om at det etableres og innføres en internkontroll for personvern (GDPR). Internkontrollen skal inneholde nødvendige prosesser og rutiner for lovlig og forsvarlig behandling av personopplysninger. Internkontrollen skal inngå i den generelle virksomhetsstyringen. Det er et lederansvar at en internkontroll for personvern (GDPR) etableres og innføres (praktiseres). Internkontrollen skal dokumenteres, jf. punkt 12 i policyen. Øvrige krav i punktene 6-11 i policyen spesifiserer nærmere hvilke oppgaver som inngår i en slik internkontroll.
Praktisering av kravene	Hos median-institusjonen er status for etablering og innføring (praktisering) av internkontroll for personvern (GDPR) omtrent den samme som for ledelsessystem for informasjonssikkerhet. Det betyr at median-institusjonen har: • etablert og dokumentert sin internkontroll for personvern (GDPR), • internkontrollen er delvis innført i de ulike delene av kjernevirksomheten (forskning, undervisning, formidling og administrasjon), • internkontrollen er forankret hos toppledelsen og styret, • det er opprettet et koordinerende organ for innføring og videreutvikling av internkontrollen (forum/nettverk for informasjonssikkerhet og personvern). Som når det gjelder ledelsessystem for informasjonssikkerhet, er internkontrollen – og oppgavene som inngår i den – ikke godt nok kjent og innført (praktisert) i hele organisasjonen, spesielt på enhetsnivå.
Samsvar og avvik	Median-institusjonen overholder i noen grad de kravene som policyen stiller til etablering og praktisering av internkontroll for personvern (GDPR). Manglende innføring (praktisering) av internkontrollen i hele organisasjonen (alle deler av kjernevirksomheten) er et avvik fra kravene i departementets policy nevnt ovenfor, jf. spesielt punkt 6b.

	Særlig på enhetsnivå mangler median-institusjonen noe av den kapasiteten og kompetansen som kreves for å utføre viktige personvernoppgaver.

Behandlingsprotokoll	
Krav i policyen	Punkt 6c i departementets policy krever at det etableres og vedlikeholdes en oversikt over hvilke behandlinger av personopplysninger som institusjonen er rettslig ansvarlig for (behandlingsprotokoll). Behandlingsprotokollen skal gi en dekkende oversikt over hva institusjonen er behandlingsansvarlig for.
Praktisering av kravene	Median-institusjonen har delvis oversikt over hvilke behandlinger av personopplysninger som institusjonen er rettslig ansvarlig for. Behandlingsprotokollen er mest fullstendig innen forskning, inkludert studentforskning. Her benyttes NSD (nå Sikt) sitt meldingsarkiv som protokoll. Median-institusjonen har også oversikt over behandlinger av personopplysninger i sentralt forvaltede digitale systemer og tjenester. Behandlingsprotokollen er mer mangelfull for digitale systemer og tjenester som ikke forvaltes sentralt. Protokollen kan også være noe mangelfull i undervisning og i deler av administrasjonen.
Samsvar og avvik	Median-institusjonen overholder i noen grad de kravene som policyen stiller til etablering og vedlikehold av behandlingsprotokoll. Mangelfull protokoll for deler av virksomheten, spesielt for digitale systemer og tjenester som forvaltes på enhetsnivå, er et avvik fra kravene i policyens punkt 6c.

Personvernrettigheter (GDPR)	
Krav i policyen	Punkt 7 i departementets policy krever at personvernrettighetene til de registrerte (ansatte, studenter, deltakere i forskningsprosjekter, osv.) blir ivaretatt. Det skal etableres prosesser og rutiner som sørger for at rettighetene blir respektert, for eksempel når det gjelder retten til informasjon, innsyn retting og sletting, jf. punkt 7a.

Praktisering av kravene	Median-institusjonen har etablert tilfredsstillende prosesser og rutiner for ivaretakelse av de registrertes rettigheter.
Samsvar og avvik	Median-institusjonen etterlever de kravene som policyen stiller til ivaretakelse av de registrertes personvernrettigheter.

Personvernombud	
Krav i policyen	Punkt 8 i departementets policy krever at det opprettes personvernombud hos universitetene og høgskolene. I punk 8b forventes det at personvernombudet har de ressursene og den kompetansen som er nødvendig for å utføre sine oppgaver på hensiktsmessige måter. Personvernombudet skal være uavhengig, og ikke underlagt ledelsens instruksjonsmyndighet i sin rolle som ombud.
Praktisering av kravene	Median-institusjonen har utnevnt et personvernombud. Ombudsrollen utgjør omkring 60 prosent[11] av en hel stilling. Hos median-institusjonen ivaretar personvernombudet sine lovpålagte oppgaver, blant annet ved å bistå ved eller legge til rette for gjennomføring av personvernkonsekvensvurderinger (DPIA), jf. punkt 9 i policyen. Ombudet mottar få henvendelser fra de registrerte (studenter, ansatte, forskningsdeltakere, osv.) om bruk av personvernrettigheter. Median-institusjonen benytter personvernombudet til enkelte oppgaver som ligger utenfor ombudsrollen.
Samsvar og avvik	Median-institusjonen etterlever flere av kravene som policyen stiller til personvernombud. Det kan stilles spørsmål ved om ombudet har tilfredsstillende muligheter til faglig oppdatering/kompetanseheving, jf. policyens punkt 8b. Bruk av personvernombudet til oppgaver som ikke ligger til ombudsrollen, er et avvik fra kravene i policyens punkt 8.

[11] Dette er gjennomsnittlig stillingsprosent, se også «Ressurser (årsverk)» ovenfor.

Kompetanse, opplæring og bevissthet	
Krav i policyen	Punkt 11 i departementets policy krever at ledere og medarbeidere med roller i arbeidet med informasjonssikkerhet og personvern har den kompetansen de trenger for å ivareta sitt ansvar og sine oppgaver. Det forutsetter at disse lederne og medarbeiderne får den opplæringen som er nødvendig. I punkt 11a og 11c forventes det at ledere, medarbeidere og studenter informeres om og bevisstgjøres problemstillinger knyttet til informasjonssikkerhet og personvern, inkludert trusler mot IKT-sikkerheten.
Praktisering av kravene	Median-institusjonen har gjennomført egnede tiltak for å øke bevisstheten om personvern og informasjonssikkerhet hos ledere, medarbeidere og studenter. Det skjer i særlig grad i forbindelse med «Nasjonal sikkerhetsmåned» (nano-læringskurs). Median-institusjonen har iverksatt enkelte rollespesifikke opplærings- og kompetansehevende tiltak. Tiltakene er primært rettet mot system- eller tjenesteeiere. De rollespesifikke opplærings- og kompetansehevende tiltakene har et relativt begrenset omfang. Median-institusjonen mangler ressurser til å dekke opplæringsbehovet i organisasjonen.
Samsvar og avvik	Median-institusjonen etterlever de krav som policyen stiller til generell bevisstgjøring. Mangelfull rollespesifikk opplæring, spesielt rettet mot ledere eller medarbeidere med viktige oppgaver innen informasjonssikkerhet og personvern, er et avvik fra kravene i departementets policy, jf. spesielt punkt 11b.

Sektorprofilen – oppsummert

Når vi oppsummerer den mest typiske (vanlige) etterlevelsen for hver av de 13 kravene i policyen for informasjonssikkerhet og personvern som er drøftet i denne rapporten, får vi en samlet sektorprofil.

Sektorprofilen presenteres nedenfor. Den sammenfatter status med hensyn til samsvar og avvik hos median-institusjonen.

Informasjonssikkerhetshendelser: Det påvises ikke avvik fra policyen hos median-institusjonen. Hver institusjon må selv vurdere om omfanget av og typer hendelser og brudd på informasjonssikkerhetsområdet er akseptabelt.

Ressurser (årsverk): Det påvises ikke avvik fra policyen hos median-institusjonen. Avvik fra andre krav i policyen kan imidlertid indikere at ressursinnsatsen bør styrkes.

Ledelsessystem for informasjonssikkerhet: Median-institusjonen overholder i noen grad de kravene som policyen stiller. Lokale enheter (fakulteter, institutter) mangler noe av den kapasiteten og kompetansen som kreves for å utføre viktige oppgaver.

Organisering av arbeidet: Median-institusjonen overholder i hovedsak kravene i policyen som gjelder etablering og dokumentasjon av sikkerhetsorganiseringen. Iverksetting (praktisering) av den beskrevne organiseringen er noe mangelfull, spesielt på fakultets- og instituttnivå.

Toppledelsen og styret: Median-institusjonen overholder i hovedsak de kravene som policyen stiller. Det kan stilles spørsmål ved om styret ikke bør utøve sterkere kontroll med arbeidet.

Risikostyring (vurderinger og tiltak): Median-institusjonen overholder i noen grad de kravene som policyen stiller. Systematikken i og omfanget av risikostyringen er noe mangelfull utenfor IT-avdelingen/seksjonen.

Tjenesteutsetting (databehandlere): Median-institusjonen overholder i noen grad de krav som policyen stiller. Det kan være avvik når det gjelder bruk av databehandlere på fakultets- og instituttnivå og ved overføringer av personopplysninger til tredjeland. Oppfølgingen av og kontrollen med databehandlere er mangelfull.

Hendelseshåndtering – beredskap og kontinuitet: Median-institusjonen overholder i noen grad de kravene som policyen stiller. Den mangler tiltakskort for enkelte digitale sikkerhetshendelser og planer for opprettholdelse av kritiske oppgaver.

Internkontroll for personvern (GDPR): Median-institusjonen overholder i noen grad de kravene som policyen stiller. Fakulteter og institutter mangler noe av den kapasiteten og kompetansen som trengs for å utføre viktige personvernoppgaver.

Behandlingsprotokoll: Median-institusjonen overholder i noen grad de kravene som policyen stiller. Protokollen er mangelfull for deler av virksomheten, spesielt på fakultets- og instituttnivå.

Personvernrettigheter (GDPR): Median-institusjonen overholder de kravene som policyen stiller.

Personvernombud: Median-institusjonen overholder i hovedsak de kravene som policyen stiller. Personvernombudet har begrensede muligheter til faglig oppdatering/kompetanseheving. Ombudet benyttes også til oppgaver som ligger utenfor rollen.

Kompetanse, opplæring, bevissthet: Median-institusjonen overholder kravene som policyen stiller til generell bevisstgjøring. Den rollespesifikke opplæringen (av ledere eller medarbeidere med viktige oppgaver innen informasjonssikkerhet og personvern) er noe mangelfull.

Vedlegg 1:
Institusjonene og virksomhetene som omfattes av departementets policy for informasjonssikkerhet og personvern

Statlige universiteter og høgskoler

- Arkitektur- og designhøgskolen i Oslo.
- Høgskolen i Innlandet.
- Høgskolen i Molde - Vitenskapelig høgskole i logistikk.
- Høgskulen i Volda.
- Høgskolen i Østfold.
- Høgskulen på Vestlandet.
- Kunsthøgskolen i Oslo.
- Nord universitet.
- Norges Handelshøyskole.
- Norges idrettshøgskole.
- Norges miljø- og biovitenskapelige universitet.
- Norges musikkhøgskole.
- Norges teknisk-naturvitenskapelige universitet.
- OsloMet – storbyuniversitetet.
- Samisk høgskole.
- Universitetet i Agder.
- Universitetet i Bergen.
- Universitetet i Oslo.
- Universitetet i Stavanger.
- Universitetet i Sørøst-Norge.
- Universitetet i Tromsø - Norges arktiske universitet.

Øvrige forvaltningsorganer og selskaper

- De nasjonale forskningsetiske komiteene.
- Nasjonalt organ for kvalitet i utdanningen.
- Norges forskningsråd.
- Norsk utenrikspolitisk institutt.
- Sikt – kunnskapssektorens tjenesteleverandør.
- Simula Research Laboratory.
- Universitetssenteret på Svalbard.
- Direktoratet for høyere utdanning og kompetanse (styringsansvaret ligger hos Kunnskapsdepartementet).

Direktoratet for
høyere utdanning
og kompetanse

post@hkdir.no hkdir.no