Informasjon om eksamen

UiO : Institutt for informatikk
Det matematisk-naturvitenskapelige fakultet

Avsluttende eksamen i IN5080 Sikkerhets- og risikostyring (vår 2025).

Dato og tidspunkt: **12. juni 2025, kl.15:00 - 19:00 (4 timer).**

Ingen hjelpemidler er tillatt.

Merk følgende:

- Oppgavene i denne eksamen har 9 deler som tilsvarer 10 av forelesningene i emnet.
- Det er mulig å oppnå totalt 112 poeng (= 100%).
- Man kan navigere frem og tilbake mellom oppgavene.
- Skåring for hver oppgave angis eksplisitt. I flervalgsoppgaver kan det gis negative poeng for feil svar/valg, men total poengsum for hele oppgaven er minimum 0 (selv om summen over alle svarene er negativ).
- Vær kortfattet når du skriver tekst som svar på en tekstoppgave. Svar kan skrives på norsk/svensk/dansk eller engelsk.
- I navigasjonslinjen nederst på skjermen indikeres fullførte oppgaver med blå søyler.

Lykke til!

Grunnleggende begreper

1 Betydninger av "usikkerhet"

I setningen nedenfor brukes ordet "usikkerhet" på en upresis måte i tre ulike betydninger:
Etter en rekke uforklarlige cyberhendelser med en bestemt biltype som har hatt fatale konsekvenser, har vi forsøkt å finne årsaken. Selv om vi har noen hypoteser om kilden til digital ***usikkerhet****, hersker det fremdeles stor* ***usikkerhet*** *om hva årsaken kan være. Inntil vil har løst problemet vil det derfor skape stor* ***usikkerhet*** *i trafikken å bruke denne biltypen.*
Fyll inn tre ulike presise begreper i samme setning nedenfor. I ett av feltene skal det fremdeles stå "usikkerhet".
Poeng: 1p for hver riktig, 0p for feil eller ubesvart. Maks 3p.

Etter en rekke uforklarlige cyberhendelser med en bestemt biltype som har hatt fatale konsekvenser, har vi forsøkt å finne årsaken. Selv om vi har noen hypoteser om kilden til digital [ ], *hersker det fremdeles stor*

[ ] *om hva årsaken kan være. Inntil vil har løst problemet vil det derfor skape stor*

[ ] *i trafikken å bruke denne biltypen.*

Maks poeng: 3

2 Ansvar

Begrepet "ansvar" er tvetydig på norsk.
a) Beskriv kort de to vanligste betydningene av begrepet "ansvar". (1p for hver korrekt, maks 2p)
b) Hvilke to ulike engelske begreper oversettes vanligvis til "ansvar". (0,5p for hver korrekt, maks 1p)
Skriv korte svar nedenfor.

Format

Words: 0

Maks poeng: 3

3 Krav om informasjonssikkerhet

Virksomheter implementerer sikkerhetstiltak som er nødvendige eller som anses egnet til å redusere risiko. Nevn de tre viktigste typer **kilder** til krav om informasjonssikkerhet, som danner grunnlag for å velge sikkerhetstiltak.
Poeng: 1p for hver kilde, maks 3p.
Nevn de tre viktigste typer kilder

Maks poeng: 3

i Del 2: Personvern

4 Behandlingsgrunnlag

Se GDPR artikkel 6, nummer 1 om behandlingsgrunnlag.

For hver type av personopplysning må den behandlingsansvarlige virksomhet ha et gyldig behandlingsgrunnlag. For hvert case beskrevet nedenfor, angi om, eller hvordan behandlingen kan gjøres lovlig gjennom et passende behandlingsgrunnlag med en av bokstavene fra a) til f) i art.6 nr.1. Begrunn valget av bokstav, eller mangel på passende bokstav, i hvert case.

Case 1: Et firma selger varer på nett. Innsamling og behandling av kundedata er nødvendig for å gjennomføre salg og sende varer til kunden. Personopplysninger som lagres og behandles er navn, leveringsadresse og kredittkortnummer (ved betaling med kort).

Poeng: 1 poeng for riktig bokstav (hvis mulig) og forklaring, maks 1p.

Angi bokstav hvis behandlingen kan gjøres lovlig, og gi en kort begrunnelse.

Case 2: En virksomhet må oppgi lønnsinformasjon om ansatte til Skatteetaten for personbeskatning og for beregning av trygderettigheter. Personopplysninger som virksomheten lagrer og behandler er personnummer og lønnsinformasjon.

1 poeng for riktig bokstav (hvis mulig) og forklaring, maks 1p.

Angi bokstav hvis behandlingen kan gjøres lovlig, og gi en kort begrunnelse.

Case 3: En virksomhet har behov for å overvåke ansattes bruk av internett for ved hjelp av KI å kunne vurdere ansattes effektivitet i arbeidet. Vurderingene som er obligatorisk skal gjøres tilgjengelig for den ansattes leder og for den ansatte. Informasjon som samles inn og behandles er navn på web-domener som aksesseres og mottageradresser for e-poster som sendes. Tidspunkt for de ovenfor nevnte datapunktene lagres også.

1 poeng for riktig bokstav (hvis mulig) og forklaring, maks 1p.

Angi bokstav hvis behandlingen kan gjøres lovlig, og gi en kort begrunnelse.

Case 4: En virksomhet har behov for å opprettholde sterk cybersikkerhet ved å overvåke bruken av de ansattes IT-enheter for å avdekke skadevare og oppkobling mot skadelige nettsteder. Informasjon som samles inn og behandles er navn på applikasjoner som kjøres på IT-enhetene, IP-addresser som enhetene kommuniserer med, og hashverdi av filer som lastes ned. Tidspunkt for de ovenfor nevnte datapunktene lagres også. Denne informasjonen brukes av automatiserte verktøy som trigger alarm om mulig cyberangrep for igangsetting av respons.

1 poeng for riktig bokstav (hvis mulig) og forklaring, maks 1p.

Angi bokstav hvis behandlingen kan gjøres lovlig, og gi kort begrunnelse.

Maks poeng: 4

5 Berettigede interesser

Se GDPR Artikkel 6.1 om behandlingsgrunnlag.
For å kunne vurdere om bokstav f) (berettigede interesser) danner behandlingsgrunnlag kan det gjennomføres en test bestående av å svare på tre spørsmål. Hvilke tre spørsmål utgjør testen for å avgjøre om bokstav f) danner behandlingsgrunnlag?
1 poeng for hvert riktige spørsmål, maks 3p.
Skriv ditt svar her

Maks poeng: 3

6 Overføringsgrunnlag

1) Hva menes med begrepet "overføringsgrunnlag"? (1 poeng)
Skriv ditt svar her

2) Hva menes med begrepet "adekvansbeslutning"? (1 poeng)
Skriv ditt svar her

3.a) Hva var Schrems-II-dommen (0,5p)?
3.b) Hvilken ny avtale er inngått mellom EU og USA som følge av Schrems-II-dommen? (0,5p)
Skriv ditt svar her

4) Må norske virksomheter gjøre spesielle vurderinger før de kan behandle personopplysninger hos en amerikansk skyleverandør? Begrunn svaret. (1 poeng)
Skriv ditt svar her

Maks poeng: 4

7 DPIA

Når en virksomhet utfører DPIA, er det på en måte som *"å sette bukken til å passe havresekken"*. På engelsk kan det uttrykkes som *"to let the fox guard the henhouse"*. Forklar denne analogien.

1p for meningsfull forklaring.

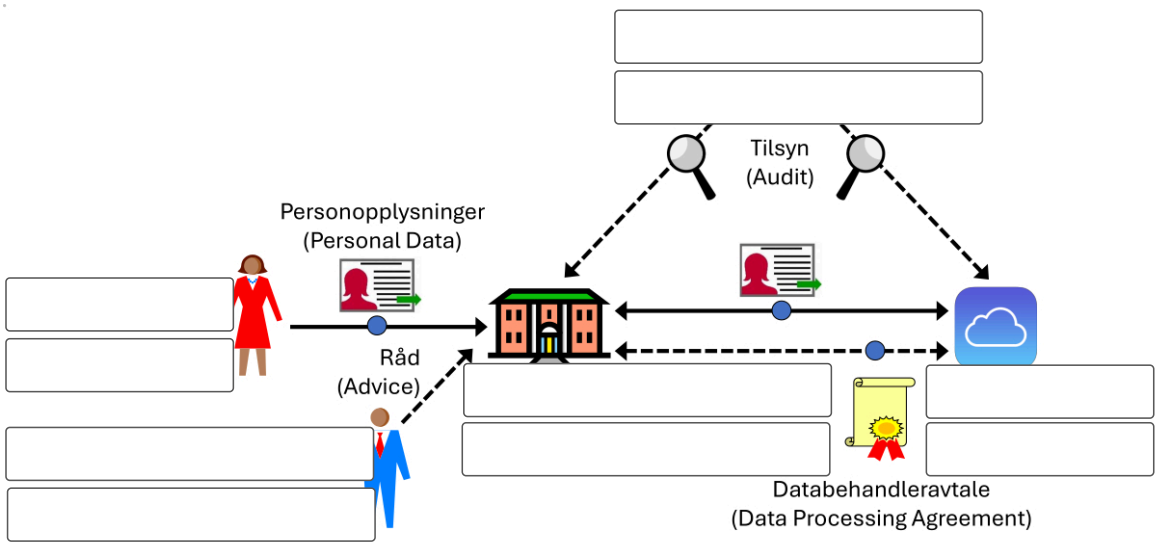
Skriv ditt svar her

Maks poeng: 1

8 Roller i GDPR

Figuren viser fem ulike roller/aktører som er beskrevet i GDPR. For hver rolle er det to tekstfelt. Fyll inn det norske begrepet for rollen i det øverste teksfeltet, og det engelske begrepet i det nederste tekstfeltet.

Poeng: 0,3p for hver korrekt, og 0p for hver feil eller ubesvart. Maks 3p, minimum 0p.



Maks poeng: 3

i Del 3: CISO

9 Holistisk tilnærming

En holistisk tilærming til informasjonssikkerhetsledelse består av personlig utvikling, ledelse, informasjonssikkerhet og kombinere ferdighetene.

Gi et eksempel på en scenario hvor det er nyttig å kunnskap om personlig utvikling?

Poeng: Maks 2p.

Skriv ditt svar her

Gi et eksempel på en scenario hvor det er nyttig å kunnskap om ledelse?

Maks 2p.

Skriv ditt svar her

Gi et eksempel på hvorfor det **IKKE** er tilstrekkelig for en CISO å kun mestre informasjonssikkerhet, men at man også må kunne kombinere fagfeltene personlig utvikling, ledelse og informasjonssikkerhet.

Maks 2p.

Skriv ditt svar her

Maks poeng: 6

10 De fire P-ene

Din leder, som er CISO, har innkalt deg til et møte med en leverandør. Formålet med møtet er å vurdere en "revolusjonerende" sikkerhetsløsning fra denne leverandøren.

Fordelen med sikkerhetsløsningen er at den samler og vurderer trusselvurderinger og nyheter om alle sikkerhetstrusler basert på AI, noe som gjør at løsningen kan oppdage og håndtere sikkerhetstrusler automatisk.

Siden du og CISO arbeider i en virksomhet med samfunnskritisk funksjon, kan leverandøren tilby gode rabatter hvis dere signerer avtalen i løpet av uken.

Hvordan kan du bruke de fire P-ene (People, Process, Product og Partner) til å utfordre om leverandøren har hensyntatt alle typer kostnader?

Poeng: Maks 4p.

Beskriv de fire P-ene.

Maks poeng: 4

11 Organisere sikkerhet

For at en CISO skal kunne organisere sikkerhetsarbeidet i virksomheten, er det en fordel å ha kompetanse i prosessutvikling, ettersom sikkerhetsarbeid består av prosesser. En moden sikkerhetsprosess inkluderer elementene: mål/prinsipper, måling, roller/ansvar, modellering, dokumentering og verktøystøtte.

Forklar hvorfor ethvert sikkerhetsarbeid og -prosesser bør starte med mål og prinsipper.

Maks 2 poeng.

Skriv ditt svar her

Virksomheten har besluttet at all form for testing av funksjonalitet skal gjennomføres i et testmiljø. Svar på deloppgavene under:

1. Beskriv en enkelt måling som kan være nyttig å samle inn.
2. Beskriv en metrikk som kan være nyttig å samle og rapportere til ledelsen
3. Hvorfor bør en alle metrikker ha en terskelverdi og gi et eksempel på terskelverdi som kan være passende for deloppgave 2, altså metrikken du rapporterte til ledelsen.

Maks 3 poeng.

Skriv ditt svar her

Maks poeng: 5

12 Samarbeid

Du har fullført mastergraden din og fått en ny jobb. Du har fått i oppdrag å integrere sikkerhetskrav i Human Resource (HR)-avdelingen i forbindelse med ansettelsesprosessen.

Du oppdager at lederen for HR-avdelingen er generelt negativ til informasjonssikkerhet. Du ønsker å bygge gjensidig respekt og godt samarbeid.

Velg **2** prinsipper for å skape respekt, og forklar hvordan du kan anvende dem i praksis for å oppnå gjensidig respekt og godt samarbeid.

Maks 4 poeng.

Skriv ditt svar her

Maks poeng: 4

i Del 4: Cyberberedskap

13 Beredskapsprinsipper

En hendelse som berører nettverk og kommunikasjon har oppstått. Det operative sikkerhetsmiljøet ønsker å påta seg oppgaven, men fagmiljøet for nettverk og kommunikasjon protesterer og mener dette er et **BRUDD** på prinsippet om?:

Maks 1 poeng.

Velg ett alternativ

- Nærhet
- Ansvar
- Samvirke
- Likhet

En hendelse som berører backup har inntruffet, men fagmiljøet for backup har ikke etablert en beredskapsplan.

Dette er **BRUDD** på prinsippet om?:

Maks 1 poeng.

Velg ett alternativ

- Samvirke
- Nærhet
- Likhet
- Ansvar

Fagmiljøet for backup har behov for bistand fra en underleverandør, men siden de ikke har etablert en samarbeidsavtale, kan ikke underleverandøren bistå.

Dette er **BRUDD** på prinsippet om?:

Maks 1 poeng.
Velg ett alternativ:

- Ansvar
- Nærhet
- Samvirke
- Likhet

Maks poeng: 3

14 BCP og DRP

Det har oppstått strømbrudd, men virksomhetens SOC (Security Operations Center) blir ikke rammet, ettersom de har UPS (Uninterruptible Power Supply), også kjent som avbruddsfri/backup strøm. Dette betyr at SOC-miljøet vil kunne være operativt i 4 timer før UPS-en går tom.

Hvilket type planverk bør de iverksette før UPS-en blir tom?

Maks 1p, min 0p.
Velg ett alternativ:

- Business continuity plan (BCP)
- Disaster recover plan (DRP)

Maks poeng: 1

15 RTO, RPO og MTD

Du oppdager at virksomheten har ikke definert hvor raskt en tjeneste skal være tilgjengelig igjen ved driftsavbrudd. Noe som gjør det vanskelig for deg å vurdere om sikkerhetstiltakene er tilstrekkelig. Dette er et eksempel på at virksomheten har ikke definert:

Maks 1p
Velg ett alternativ

- Varslingskriterier
- Recovery point objective (RPO)
- Recovery time objective (RTO)
- Maximum tolerable downtime (MTD)

Du oppdager at virksomheten har ikke definert hvor mye data og forretningstransaksjoner de er villig til å miste. Noe som gjør det vanskelig for deg å vurdere om sikkerhetstiltakene er tilstrekkelig. Dette er et eksempel på at virksomheten har ikke definert:

Maks 1p
Velg ett alternativ:

- Varslingskriterier
- Maximum tolerable downtime (MTD)
- Recovery time objective (RTO)
- Recovery point objective (RPO)

Maks poeng: 2

16 Generelt beredskap

Indiker for hvert utsagn nedenfor om det er riktig eller feil.
0,5p for hvert riktig valg, 0p for feil eller ubesvart. Maks 3p, min 0p.
Velg om utsagnet er riktig eller feil.

	Riktig	Feil
1. En sikkerhetshendelse omhandler kun trusler (tilsiktede handlinger)	○	○
2. En sikkerhetshendelse har kun en økonomisk konsekvens	○	○
3. En cyberberedskapsplan er en del av virksomhetens beredskapsplan	○	○
4. Business Continuity Plan kan sammenlignes med en nødrutine	○	○
5. Hvem som helst kan aktivere beredskapsplanen	○	○
6. Håndtering av hendelser skal alltid håndteres på lavest mulig nivå (nærhetsprinsippet).	○	○

Maks poeng: 3

i Del 5: Cybersikkerhetsstyring

17 ISO-standarder for informasjonssikkerhet

1) Hva handler standarden ISO/IEC 27000 om? (0,5 poeng)
Skriv ditt svar her.

2) Hva handler standarden ISO/IEC 27001 om? (0,5 poeng)
Skriv ditt svar her.

3) Hva handler standarden ISO/IEC 27002 om? (0,5 poeng)
Skriv ditt svar her.

4) Hvilken av ovennevnte standardene danner grunnlag for sertifisering? (0.5p poeng).
Skriv ditt svar her.

Maks poeng: 2

18 Revisor for LSIS

Oppgave 1: Hva står ISMS for? (1p) Er LSIS og ISMS forskjellig? Hvis så, forklar forskjellen. (1p)
Poeng: Maks 2p.
Skriv ditt svar her

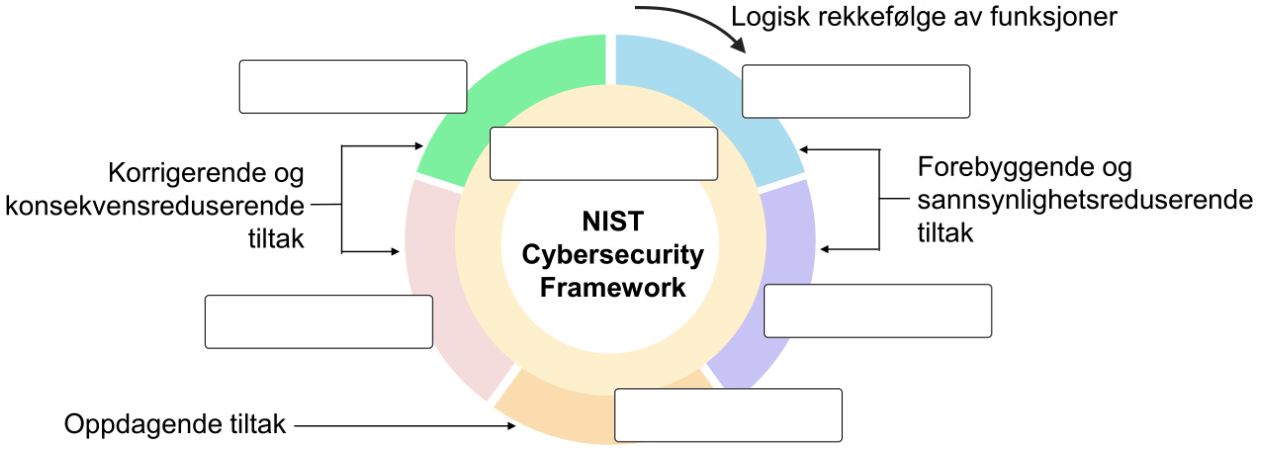
Oppgave 2:
Anta at du jobber som revisor av LSIS i henhold til ISO/IEC 27001 LSIS - Krav.
I denne oppgaven skal du revidere UiOs LSIS i henhold til kravene i ISO/IEC 27001 punkt 4.3. *Bestemme omfanget av ledelsessystemet for informasjonssikkerhet*.
På dokumentet vises kapittel 4 *Organisasjonens kontekst* i ISO/IEC 27001, og kapittel 1.3 *Virkeområde* i UiOs LSIS.
Merk at "omfang" i ISO/IEC 27001 har samme betydning som "virkeområde" i UiOs LSIS.
Vurder og beskriv i hvilken grad UiOs LSIS samsvarer med hvert krav i ISO/IEC 27001 kapittel 4.3.
Poeng: Maks 4p.

Skriv din vurdering av samsvar med krav i kapittel 4.3

Maks poeng: 6

19 NIST Cybersecurity Framework

Figuren viser en illustrasjon av NIST Cybersecurity Framework. Hvert element i den ytterste sirkelen representerer en sikkerhetsfunksjon. Den innerste sirkelen representerer en ny funksjon som ble lagt til i CSF 2.0 fra 2024. Fyll inn i hvert tekstfeltet det begrepet som beskriver hver funksjon. Du kan skrive begrepet på engelsk eller norsk.
Poeng: 0,5p for hver korrekt, og 0p for hver feil eller ubesvart. Maks 3p, minimum 0p.



Maks poeng: 3

20 Kategorisering av sikkerhetstiltak

Standarder og rammeverk kategoriserer sikkerhetstiltak på ulike måter, f.eks. domener (organisatoriske, fysiske, personell-, og teknologiske tiltak), funksjoner (preventive, detektive, og korrektive tiltak), og driftsoperasjoner (tiltak for kryptering, autentisering, sikkerhetskopi, inntrengingsdeteksjon, hendelsesrespons, osv.). Angi hvilken type kategorisering som brukes i standardene/rammeverkene listet til venstre nedenfor.

Poeng: 0,5p for hver riktig, -0,5p for hver feil, 0p for ubesvart, maks 2p, min 0p.

Velg riktig kategorisering:

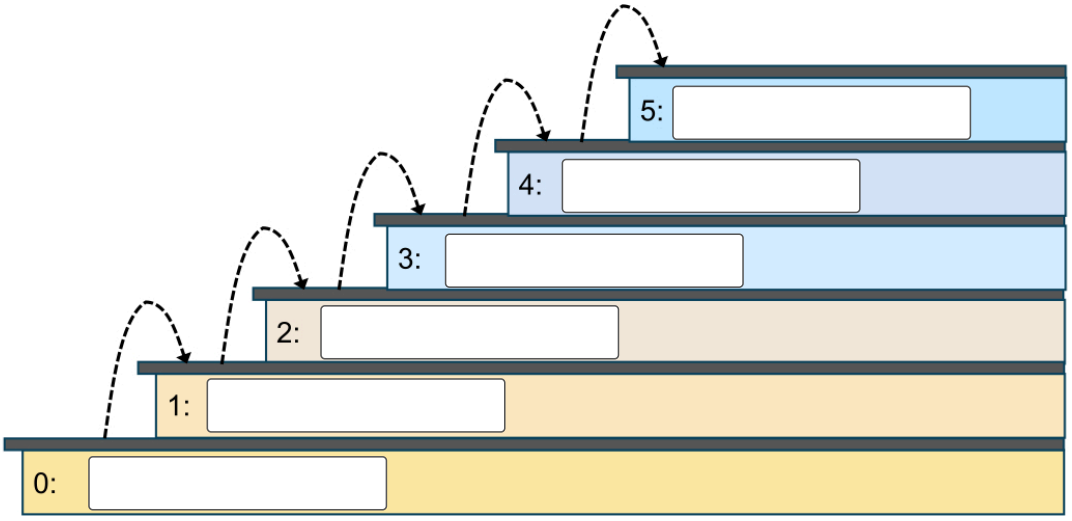
	Domener	Operasjoner	Funksjoner
CIS Controls	○	○	○
NIST Cybersecurity Framework	○	○	○
ISO/IEC 27002	○	○	○
NSMs grunnprinsipper for IKT sikkerhet	○	○	○

Maks poeng: 2

21 Modenhet i styring av cybersikkerhet

Figuren viser modenhetsnivår for styring av cybersikkerhet etter CMMI-modellen. For hvert modenhetsnivå fyll inn i tekstfeltet det begrepet som beskriver nivået.

Poeng: 0,5p for hver korrekt, og 0p for hver feil eller ubesvart. Maks 3p, minimum 0p.



Maks poeng: 3

22 CMMI modenhetsaspekter

Spørsmåle nedenfor er relatert til CMMI modenhesmodellen i forrige oppgave.

Spørsmål 1: Hva er det viktigste forskjellen mellom CMMI modenhetsnivå 2 og 3?
Poeng: Maks 1p.
Nevn den viktigste forskjellen

Spørsmål 2: Hva er det viktigste forskjellen mellom CMMI modenhetsnivå 3 og 4?
Poeng: Maks 1p.
Nevn den viktigste forskjellen

Spørsmål 3: Hva er det viktigste forskjellen mellom CMMI modenhetsnivå 4 og 5?
Poeng: Maks 1p.
Nevn den viktigste forskjellen

Maks poeng: 3

i Del 6: Strategi, tilsyn og revisjon

23 Rammebetingelser for strategi

Nevn fire relevante rammebetingelser som vil påvirke virksomhetens strategi for cybersikkerhet?
Poeng; 0,5p poeng for hver relevante rammebetingelse. Maks 2p.

Nevn fire rammebetingelser

Maks poeng: 2

24 Bruk av NSMs grunnprinsipper i revisjon

NSMs grunnprinsipper for IKT-sikkerhet kan brukes som grunnlag i revisjon. Nevn to måter NSMs grunnprinsipper danne utgangspunkt for revisjon.

Poeng: 1 poeng for hver riktig måte, maks 2 poeng.

Nevn to måter å bruke NSMs grunnprinsipper i revisjon

Maks poeng: 2

25 Krav til å være revisor

Nevn hvilke tre krav som gjelder for å være revisor.

Poeng: 1p for hvert korrekte krav, maks 3p.

Nevn tre krav for å være revisor

Maks poeng: 3

26 Forskrift og veiledning

Kraftberedskapsforskriften regulerer informasjonssikkerhet i kraftforsyningen. Indiker hva som er korrekt om *forskriften* og *veiledningen* til forskriften.

Det er mulig at noen av alternativene på høyre side aldri er korrekt.

0,5 poeng for riktig, 0 for feil eller ubesvart, maks 2 poeng, min 0 poeng.

Velg korrekt alternativ.

	Forskrift	Veiledning	Begge	Ingen
Gir råd om etterlevelse	○	○	○	○
Virksomheten kan benytte alternativ	○	○	○	○
Forvaltes av NVE	○	○	○	○
Kan medføre sanksjoner å ikke følge	○	○	○	○

Maks poeng: 2

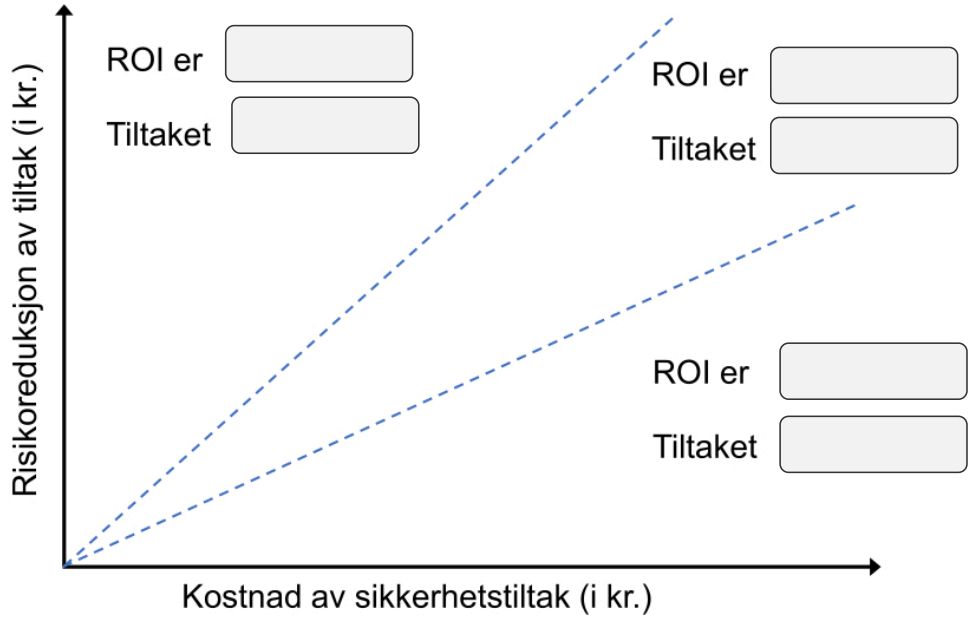
ℹ Del 7: Risikostyring

27 Risiko ROI og beslutning om tiltak

Figuren viser et diagram over risiko ROI. Flytt tekstelementene til figuren for å fylle inn riktig tekst.
Poeng: 0,5p for hver riktig tilordning, -0,5p for hver feil, 0p for manglende tilordning, maks 3p, minimum 0p.

Hjelp

nøytral	positiv	kan vurderes	bør ikke velges
negativ	bør velges		



Maks poeng: 3

28 Formel for risiko ROI

Risiko ROI (Return On Investment) er et mål på forventet lønnsomhet ved innføring av et sikkerhetstiltak. Oppgi formelen for risiko ROI i feltet nedenfor. Bruk ord/begreper for variablene i formelen.
Poeng: 2p for riktig formel. 0p for feil eller ubesvart. Maks 2p, minimum 0p.

Risiko ROI =

Maks poeng: 2

29 Risikoberegning

Tabellen nedenfor viser en risikomatrise, der cellene for risikonivåer ikke er fyllt inn.

Risikomatrise

5: Snarest						
4: Sannsynlig						
3: Mulig						
2: Usannsynlig						
1: Sjelden						
0: Aldri						
Sannsyn./Kons.	0: Ingen	1: Ubetydelig	2: Liten	3: Betydelig	4: Stor	5: Verst

Poeng: For hver oppgave nedenfor gis 0,5p for riktig, -0,5p for feil og 0p for ubesvart. Totalt maks 2p, minimum 0p.

Oppgave 1: Si om risikomatrisen over er ment å vise a) kvalitativ/ordinal risiko, b) relativ risiko, eller c) kvantitativ risiko
En risikomatrise er ment å vise

- Kvalitativ/ordinal risiko
- Relativ risiko
- Kvantitativ risiko

Oppgave 2: Si hvordan kvalitativ/ordinal risiko beregnes:
Kvalitativ/ordinal risiko beregnes

- Additivt
- Multiplikativt

Oppgave 3: Si hvordan relativ risiko beregnes:
Relativ risiko beregnes

- Additivt
- Multiplikativt

Oppgave 4: Si hvordan kvantitativ risiko beregnes:
Kvantitativ risiko beregnes

- Additivt
- Multiplikativt

Maks poeng: 2

30 Case risikovrdering

Se beskrivelsen av caset.

Oppgave 1:

Nettuniversitetet forvalter verdier som kan utsettes for sikkerhetstrusler.

Beskriv et enkelt register over to (2) verdier i Nettuniversitetet, der hver verdi er beskrevet med relevante attributter. Gjør beskrivelsen relativt generell, det er ikke nødvendig å beskrive detaljerte verdier. Det som er viktig er ikke hvilke verdier som beskrives, men hvordan de beskrives.

(Maks 2p)

Oppgave 2:

Det oppstår sikkerhetsrisikoer i den grad Nettuniversitetet sine verdier er sårbar for relevante trusler. Disse truslene skaper betydelige risikoer som må håndtres slik at restrisikoen er akseptabel. Skriv en enkel repport for risikostyring i form av risikovurdering og foreslått risikohåndtering for en (1) risiko. For utførelsen av risikovurderingen skal risikomatrisen fra forrige oppgave benyttes. Tallverdiene i de tomme cellene kan enkelt beregnes, det er ikke nødvendig å definere ord/begreper for risikonivåer. Rapporten skal inneholde:

a. Bestemmelse av nivå for akseptabel risiko. Det fins intet intet absolutt korrekt nivå, så et fornuftig nivå skal velges. (Maks 1p)

b. Beskrivelse av risikoen. Ikke bli stående fast pga. mangel på detaljer i case-beskrivelsen av Nettuniversitetet, du kan gjøre passende antagelser hvis nødvendig. Punktene (i-iii) nedenfor skal besvares.

i. I beskrivelsen av risikoen skal følgende elementer inkluderes.

- Kort beskrivelse av risikoen (trusselscenario, hvilke sårbarheter kan utnyttes i angrepet og hvilke verdier som skades) (Maks 2p)
- Sannsynlighetsvurdering (hvilke faktorer påvirker sannsynlighet?). Estimer kvalitativ sannsynlighet for hendelsen. (Maks 1p)
- Konsekvensvurdering (hvilke konsekvenser kan hendelsen få?). Estimer helhetlig kvalitativ konsekvens for hendelsen. (Maks 1p)

ii. Foreta en kvalitativ risikoanalyse ved å beregne risikonivået basert på de estimerte inputverdiene. Benytt risikomatrisen fra forrige oppgave. (Maks 1p)

iii. Foreslå en relevant måte å håndtere risikoen i den grad risikonivået ligger over nivå for akseptabel risiko. (Maks 1p)

Skriv ditt svar her

Format

Words: 0

Maks poeng: 9

Del 7: Regelverk

31 Karakteristikk av lover

Velg korrekt alternativ i beskrivelsen av sikkerhetsloven, personopplysningsloven,
og lov om digital sikkerhet.
Poeng: 0,25p for hver rijktig, -0,25p for hver feil, 0p for ubesvart. Maks 3p, minimum 0p.

En annet navn for sikkerhetsloven er Velg alternativ (NIS1/NIS2, GDPR, Cybersikkerhetsloven, (intet annet navn på loven)).

Et annet navn på personopplysningsloven er Velg alternativ (NIS1/NIS2, GDPR, Cybersikkerhetsloven, (intet annet navn)).

Et annet navn på lov om digital sikkerhet er Velg alternativ (NIS1/NIS2, GDPR, Cybersikkerhetsloven, (intet annet navn)).

Sikkerhetsloven er opprinnelig en Velg alternativ (norsk lov, EU-lov).

Personopplysningsloven er opprinnelig en Velg alternativ (norsk lov, EU-lov).

Lov om digital sikkerhet er opprinnelig en Velg alternativ (norsk lov, EU-lov).

Sikkerhetsloven omhandler Velg alternativ (tilsiktede handlinger, alle slags hendelser (all hazards)) som kan skade

Velg alternativ (vesentlige og viktige enheter, nasjonal sikkerhet og grunnleggende funksjoner, personvern, alle typer verdier).

Personopplysningsloven omhandler Velg alternativ (alle typer hendelser (all hazards), tilsiktede handlinger) som kan

skade Velg alternativ (vesentlige og viktige enheter, nasjonal sikkerhet og grunnleggende funksjoner, personvern, alle typer verdier).

Lov om digital sikkerhet omhandler Velg alternativ (tilsiktede handlinger, alle slags hendelser (all hazards)) som som kan

skade Velg alternativ (vesentlige og viktige enheter, nasjonal sikkerhet og grunnleggende funskjoner, personvern, alle typer verdier).

Maks poeng: 3

32 Regelverk fra EU

EU publiserer ulike typer regelverk som ofte gjelder for Norge.

a) Hvordan bestemmes det om et direktive eller en forordning skal gjelde for Norge? (1p)

Skriv ditt svar her

b) Hva er et EU-direktiv (directive), og hvordan implementeres et EU-direktiv i Norge? (2p)

Skriv ditt svar her

c) Hva er en EU-forordning (regulation), og hvordan implementeres en EU-forordning i Norge? (2p)

Skriv ditt svar her

Maks poeng: 5

i Del 9: Cybertrusler og håndtering

33 Cyber Kill Chain

Nevn navn på hvert trinn i cyber kill chain, med en kort forklaring av hvert trinn.
Poeng: 0,25p for korrekt navn, og 0.25p for korrekt forklaring.. Maks 3,5p, minimum 0p.

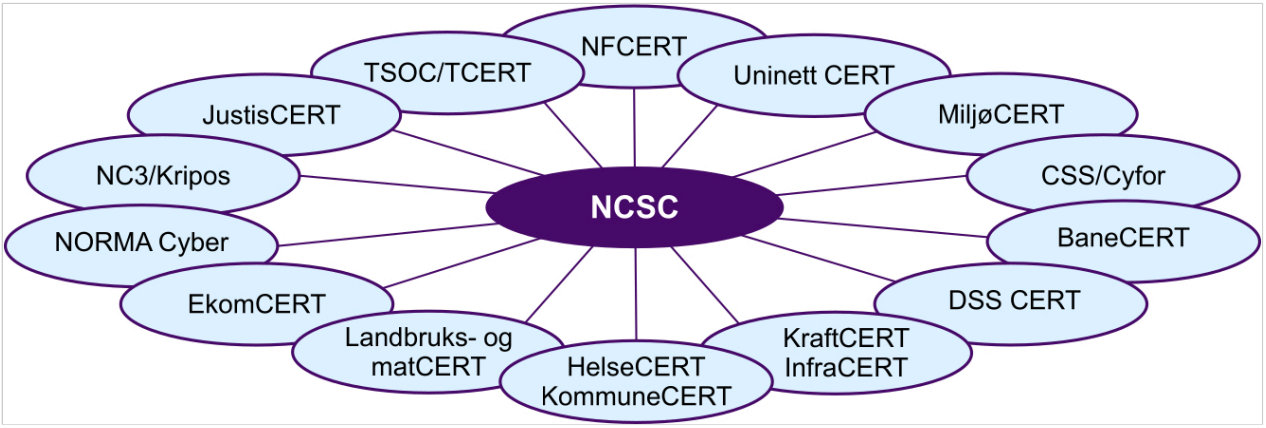
Skriv navn og forklaring på hvert trinn

Beskriv kort en relevant måte å stoppe angriper på trinn 1 i cyber kill chain.
Poeng: 0,5p for korrekt relevant måte.

Beskriv måte å stoppe trinn 1

Maks poeng: 4

34 Håndtering



Se på figuren.

Oppgage 1: Hva kalles organene som er illustrert med lyseblå ovaler, og hvilken rolle har et slikt organ?

Poeng: 1p for korrekt navn og 1p for korrekt rollebeskrivelse. Maks 2p.

Skriv navn og rolle her

Oppgave 2: Hva betyr forkortelsen i den mørkeblå ovalen, og hvilken rolle har det organet nasjonalt og internasjonalt?

Poeng: 1p for korrekt navn og 1p for korrekt rollebeskrivelse. Maks 2p.

Skriv navn og rolle her

Maks poeng: 4

i Slutt på eksamen

Question 18
Attached



Utdrag fra ISO/IEC 27001:2022 LSIS - Krav

4. Organisasjonens kontekst

4.1. Forstå organisasjonen og dens kontekst

Organisasjonen skal bestemme eksterne og interne forhold som er relevante for dens formål, og som påvirker dens evne til å oppnå tiltenkt(e) resultat(er) av sitt ledelsessystem for informasjonssikkerhet.

4.2. Forstå interessentenes behov og forventninger

Organisasjonen skal bestemme:

a) hvilke interessenter som er relevante for ledelsessystemet for informasjonssikkerhet;
b) relevante krav for disse interessentene;
c) hvilke av disse kravene som kommer til å håndteres gjennom ledelsessystemet for informasjonssikkerhet.

4.3. Bestemme omfanget av ledelsessystemet for informasjonssikkerhet

Organisasjonen skal bestemme avgrensningene og anvendeligheten av ledelsessystemet for informasjonssikkerhet for å fastslå omfanget.

Når organisasjonen bestemmer omfanget, skal den ta hensyn til:

a) de eksterne og interne forholdene nevnt i 4.1;
b) kravene nevnt i 4.2,
c) grensesnitt og avhengigheter mellom de aktivitetene som utføres av organisasjonen, og de som blir utført av andre organisasjoner.

Omfanget skal være tilgjengelig i form av dokumentert informasjon.

Utdrag fra UiOs LSIS, Kapittel 1: Innledning

1. Innledning

1.1. Om dokumentet

1.2. Oversikt over universitetets ledelsessystem for informasjonssikkerhet

1.3. Virkeområde

UiOs ledelsessystem for informasjonssikkerhet (LSIS) samler retningslinjer for alle deler av IT-sikkerhetsarbeidet, inkludert informasjonssikkerheten. Den gjelder for all IT-virksomhet på universitetet enten den skjer i regi av USIT eller av andre enheter ved universitetet.

Ledelsessystemet er således styrende for:

- Sentral og lokal IT på universitetet;
- System- og tjenesteeiere;
- Samarbeidstiltak, inkludert §1.4.4-tiltak som universitetet er vertskap for;
- Institusjoner i universitetets randsone som benytter seg av universitetets IT-tjenester og IT-infrastruktur, for eksempel stiftelser. Noen randsoneenheter er selv behandlingsansvarlige for personopplysninger. Disse kan bruke eget ledelsessystem eller være en del av dette etter nærmere avtale med UiO.

I tillegg vil relevante deler av ledelsessystemet gjøres gjeldende for USITs oppdragsvirksomhet.

Ledelsessystemet inngår som en del av dokumentasjonen av sikkerhetsarbeidet på universitetet.

1.3.1. Målgrupper

IT- og informasjonssikkerhetsarbeid omfatter hele organisasjonen, og disse dokumentene har flere målgrupper:

- Universitetets ledelse og ledelsen ved fakulteter og andre enheter;
- IT-tilsatte i sentral og lokal IT-organisasjon;
- System- og tjenesteeiere;
- Universitetets IT-brukere (ansatte, studenter og andre tilknyttede brukere).

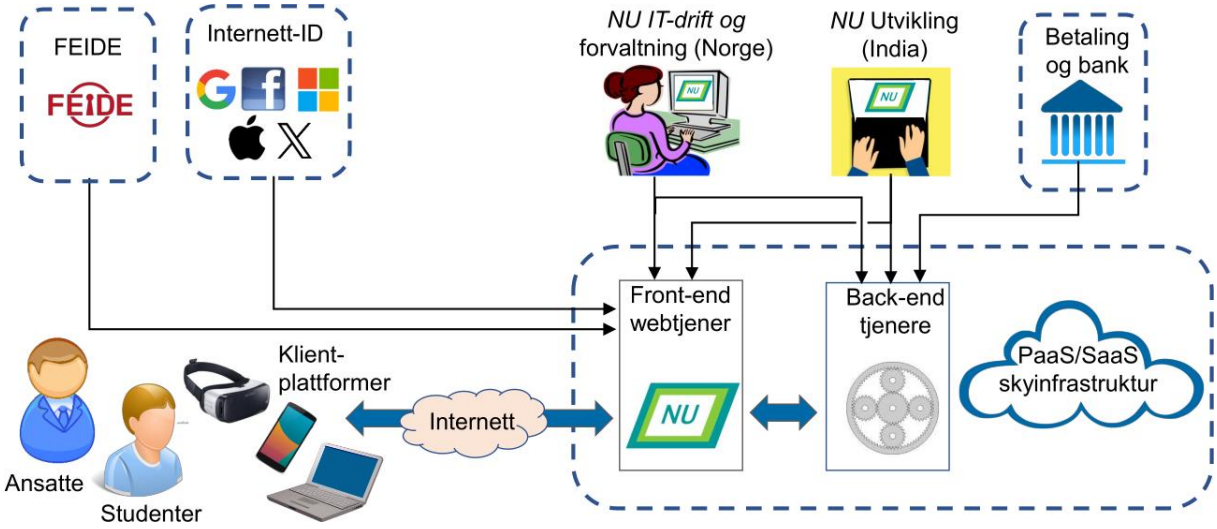
Question 30
Attached



NU : Nettuniversitetet

Nettuniversitetet (NU) (eng. Network University) er et (fiktivt) nyopprettet privat universitet der undervisning og læring utelukkende foregår online gjennom digitale plattformer.

IT-arkitekturen skal bygges på en kombinasjon av PaaS og SaaS skyløsning (Platform-as-a-Service og Software-as-a-Service. Figuren viser arkitekturen. Hvis beskrivelsen mangler detaljer som synes nødvendig for å besvare oppgavene, er det helt greit å gjøre antagelser.



Nettuniversitetet - generell nettverksarkitektur

Foreslåtte ordninger

Designerne av Nettuniversitetets digitale infrastruktur ønsker å lage en fleksibel løsning som skal være enkel for studenter og ansatte og enkel for Nettuniversitetet å utvikle, drifte og administrere. Utvikling og drift/forvaltning av løsninger er adskilt. Drift/forvaltning skal gjøres av ansatte i Norge, mens utvikling er planlagt å bli gjort fra India. For feilretting og oppdatering har utviklerne tilgang til alle skyløsningene som er i drift. Nettuniversitetet planlegger å kjøpe skytjenester fra forskjellig skyleverandører som alle ligger enten i USA eller EU/EØS. Alle foreslåtte spesifikasjoner er nummerert nedenfor.

1. Designerne foreslår at studenter og faglig/administrative ansatte skal kunne logge inn på to alternative måter:
   - Login via FEIDE med ID fra Nettuniversitetet, med passord lagret som klartekst.
   - Login med Internett-ID, f.eks. epost-adresse med autentisering utført av en IdP.

2. For utvikling skyløsningene forslår Nettuniversitetet å leie programmerere fra India, og det kreves ikke spesifikk kompetanse i applikasjonssikkerhet.

3. Utviklerne av skyløsningen, samt IT-drift og forvaltning skal bruke et enkelt selvdefinert passord for innlogging til skyplattformene. Dette kan anses som tilgang utenom vanlig brukerautentisering og tilgangskontroll som er beskrevet i punkt 1.

4. Brukerdatabasen (studenter og faglig/administrative ansatte) skal inneholde følgende:

- Navn - Ansatt-ID (for ansatte) - Studentnummer (for studenter) - Fødselsnummer (for innbyggere i Norge) - Epostadresse - FEIDE-ID	- Emne- og karakterhistorikk - Telefonnummer - Kjønn (mann/kvinne/udefinert) - Ansiktsfoto - 30 sekunder video av overkropp med tale (for avatar KI-generering)

Studenter og ansatte skal kunne delta som avatarer i virtuelle forelesninger:

5. Det skal bli gjort et 30-sekunders video-opptak av alle studenter og ansatte, som brukes til KI-generering av en virtuell avatar for hver enkelt. Student og ansatt kan opptre virtuelt i møter med automatisk oversettelse av språk. På den måten studenter og forelesere fra hele verden delta, uten begrensninger om språkkunnskap.

Nettuniversitetet er et privat kommersielt universitet, der studenter betaler for å ta kurs. Designerne ønsker følgende alternative løsninger for betaling:

6. Betaling kan gjøres med følgende løsninger:
   - Bankkort/kredittkort (+ Paypal, Apple Pay, Alipay osv.)
   - Vipps (for studenter som er innbyggere i Norge).

Når studenter og ansatte velger å benytte Internett-ID ønsker designerne å knytte Internett-ID til andre tjenesteleverandører gjennom deres OAuth-API, som tillater følgende funksjoner:

7. Nettuniversitetets studenter og ansatte kan motta info fra andre tjenestetilbydere som f.eks. læringsmateriale, profesjonelle nettverk eller virksomheter for jobbtilbud.
8. Nettuniversitetet kan utveksle studentenes lærings- og karakterhistorikk med potensielle arbeidsgivere. Nettuniversitetet kan på den måten gi anbefaling til virksomheter om hvem de burde ansette.

Designerne ønsker å la studenter gi tilbakemelding på undervisningen, som skal vises som del av informasjonen for hvert kurs på Nettuniversitetets nettsider.

9. Studenter kan bedømme kurs de har tatt med 1 – 5 stjerner.
10. Studenter kan skrive kommentarer til kurs de har tatt, der studentens navn vises.
11. Studenter kan bedømme navngitte forelesere med 1 – 5 stjerner.
12. Studenter kan skrive kommentarer om navngitte forelesere, der studentens navn vises.

Designerne foreslår en amerikansk hovedleverandør for skytjenester, og i tillegg andre skyleverandører fra USA/EU/EØS for spesifikke tjenester og funksjoner. Følgende generelle sikkerhetskrav settes til skyleverandørene:

13. Skyleverandøren er ansvarlig for nettverkssikkerhet (brannmur, IDS, logg og analyse av nettverkstrafikk) og hendelsesrespons for nettverkshendelser.
14. Skyleverandøren tar ansvar for å håndtere angrep mot selve sky-plattformen, men håndterer ikke angrep mot Nettuniversitets egne applikasjoner.

Gjennom sky-avtalene har Nettuniversitetet ansvar for spesifikke sikkerhetsaspekter:

15. Nettuniversitetet har ansvar for sikkerhet i egenutviklede applikasjoner og back-end server, men har ikke definert en spesifikk plan for hendelsesrespons eller beredskap.
16. Nettuniversitetet konfigurere nettverksinnstillinger etter behov, f.eks. hvilke porter som skal være åpne og lukket, og mot hva (Internett, andre grensesnitt, interne tjenester, etc.).
17. Web-grensesnitt sikres med serversertifikat og HTTPS.

Question 4
Attached



Utdrag fra Lov om behandling av personopplysninger (personopplysningsloven), kalt GDPR.

Artikkel 6. Behandlingens lovlighet (behandlingsgrunnlag)

1. Behandlingen er bare lovlig dersom og i den grad minst ett av følgende vilkår er oppfylt:

a. den registrerte har samtykket til behandling av sine personopplysninger for ett eller flere spesifikke formål,
b. behandlingen er nødvendig for å oppfylle en avtale som den registrerte er part i, eller for å gjennomføre tiltak på den registrertes anmodning før en avtaleinngåelse,
c. behandlingen er nødvendig for å oppfylle en rettslig forpliktelse som påhviler den behandlingsansvarlige,
d. behandlingen er nødvendig for å verne den registrertes eller en annen fysisk persons vitale interesser,
e. behandlingen er nødvendig for å utføre en oppgave i allmennhetens interesse eller utøve offentlig myndighet som den behandlingsansvarlige er pålagt,
f. behandlingen er nødvendig for formål knyttet til de berettigede interessene som forfølges av den behandlingsansvarlige eller en tredjepart, med mindre den registrertes interesser eller grunnleggende rettigheter og friheter går foran og krever vern av personopplysninger, særlig dersom den registrerte er et barn.

Nr. 1 bokstav f) får ikke anvendelse på behandling som utføres av offentlige myndigheter som ledd i utførelsen av deres oppgaver.