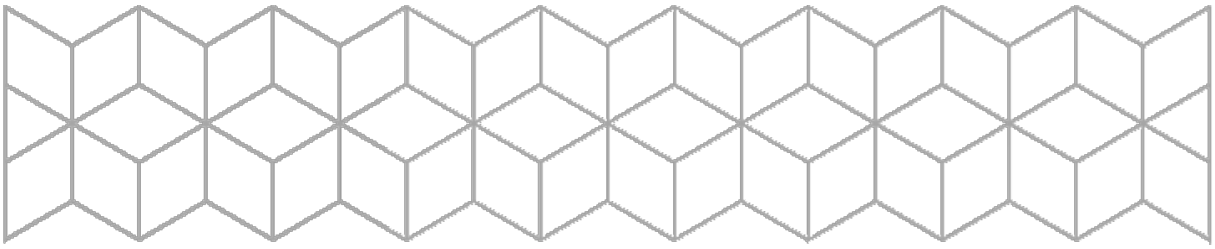
Høgskolen i Østfold

SENSORVEILEDNING

Emnekode:	**ITL27019**
Emnenavn:	**Informasjonssikkerhet**
Eksamensform:	**4 timer skoleeksamen**
Dato:	29/11-2022
Faglærer(e):	Tom Heine Nätt
Eventuelt:	



Introduksjon

I denne sensorveiledningen er det forsøkt å angi hva som kan være mulige deler av svar. Siden mange av oppgavene er svært åpne, så kan andre momenter erstatte disse. Det er heller ikke slik at det som indikeres i denne sensorveiledningen er det som skal til for å få en A. På grunn av oppgavens natur er det her opp til sensuren å avgjøre kandidatens kunnskap basert på krav i oppgaven, studentens vurderingsevne og bruk av teori og den mer overordnede beskrivelsen for karakterskalaen:

https://innsida.ntnu.no/wiki/-/wiki/Norsk/Karakterskalaen

1.1

Her bør det som minimum nevnes at sikkerhetsloven og personopplysningsloven stiller krav til internkontroll/styringssystem på hele/deler av driften.

1.2

Personvernombudet har ikke noe direkte ansvar for at personopplysningsloven følges. Ombudet skal holde oversikt over personopplysninger og behandlingsaktiviteter, påse at lovverk følges (ikke ansvar for det), gi råd, utarbeide rutiner, opplæring og informasjonsarbeid, delta i risikovurdering, være brukernes kontaktpunkt med mer.

1.3

Risikohåndtering er noe vi gjør for å unngå at en hendelse skal skje eller minimere konsekvensene av den ved hjelp av tiltak som gjøres proaktivt. Hendelseshåndtering er rutiner ag aktiviteter som gjøres når en hendelse faktisk inntreffer og gjøres i hovedsak reaktivt (unntatt planlegging/forberedelser)

1.4

I hovedsak:

- Samtykke
- Nødvendighet for å oppfylle avtale
- Nødvendighet for å oppfylle rettslig plikt
- Nødvendighet for å beskytte vitale interesser
- Nødvendighet for å utføre oppgaver i en allmenn interesse
- Nødvendighet for å ivareta legitime interesser

Merk: Her må samtykke med, ut over det bør minst to-tre av de andre med. Det er imidlertid ikke forventet at studentene gjengir de slik de er formulert i lovteksten/hos datatilsynet.

1.5

Ved pseudorandomisering vil det oppbevares en koblingsnøkkel mellom en anonym ID i datasettet og identifiserbare opplysninger i et annet datasett. De som drifter systemet har altså mulighet til å finne identiteten, og hensikten er altså å gjøre datasettet mindre verdt om det kommer på avveie. I tillegg er det ikke noen krav om at pseudorandomisert data ikke er statistisk identifiserbart (indirekte identifiserbare personopplysninger).

Bonus om studenten også nevner (ikke et krav): Kommer koblingsnøkkelen og/eller det andre datasettet med identifiserbare opplysninger på avveie er ikke lenger informasjonen anonym.

1.6

- Risikoreduserende tiltak (risk reduction)

- Risikooverføring/risikodeling (risk transfer)
- Risikofjerning (risk avoidance)
- Risikoaksept (risk retention)

Bonus om studenten nevner (ikke noe krav) at Risikoreduserende tiltak kan redusere sannsynlighet, konsekvens eller begge. Inget krav om å oppgi de både på norsk og engelsk

1.7

Security event: En hendelse som ikke har fått direkte konsekvenser. For eksempel mottak av phishing-e-post
Security incident: En hendelse som har (eller kan ha) fått direkte konsekvenser. For eksempel at noen åpnet linken i e-posten og oppgav passordet..
Inget krav om eksempler, men det kan gjøre vage forklaringer tydeligere.

1.8

Statlige, fylkeskommunale og kommunale organer samt leverandører til disse (helt eller delvis) Myndigheter kan pålegge andre aktører som håndterer informasjon, infrastruktur og tjenester av nasjon interesse å følge loven.

1.9

Kort forklart er feil det som forsorsaker hendelsen (hvordan oppstod hendelsen), mens avvik er det som forårsaket feilen (hvordan kunne feilen oppstå) . Avvik vil være feil og mangler i prosedyrer og rutiner

1.10

Vi kan sikre et høyere operasjonelt nivå når hendelsen inntreffer (dvs. får ikke like store konsekvenser/omfang som uten) og vi kan komme tilbake til normal drift raskere.

1.11

Her finnes det mange mulig inndelinger, men denne er vanlig:

- Intensjon/motivasjon
- Kapasitet/kapabilitet
- Mulighet/tilgang

Andre inndelinger som gir mening bør også gi uttelling.

1.12

Identifisering og kartlegging
Beskytte og opprettholde
Oppdage
Håndtere og gjenopprette

Så lenge kandidaten benytter ord som er dekkende, er det ikke et krav at titlene skal gjengis direkte. Det er imidlertid en bonus om de kan gjengis ordrett.

Del 2

Denne delen har ingen fasitsvar. Under er det angitt hva som er forventet at er med som et minimum, men kandidater kan likevel ha utelatt noe av dette og heller ha med andre ting som veier opp. Hva som er nivåene for hhv. A, B, C osv må avgjøres av sensor. Generelt er det imidlertid forventet at studentene kan resonere og diskutere rundt pensum, og klare å trekke tråder til andre deler av pensum enn det oppgaven direkte spør etter.

2.1

a) Her bør kandidaten som minimum beskrive hensikten av styringssystemet (få oversikt, kunne gjøre prioriteringer, lage tiltakspakker i stedet for enkelttiltak til enkelthendelser, kunne verifisere og evaluere).

b) Her bør kandidaten som minimum trekke inn lovverk (kanskje spesielt personopplysningsloven og sikkerhetsloven), ulike bransjespesifikke lover og regelverk (trenger ikke konkretisere enkeltbransjer og lovverk)

c) Her bør kandidaten drøfte evaluering, læring, øvelse i hendelseshåndtering, oppdatering av risikovurderinger og trusselbildet med mer. Et viktig moment er at for å kunne trekke ut disse positive effektene er det vesentlig at styringssystemet fanger de opp (dokumentasjon og bearbeiding) og at de inkluderes i fremtidig arbeid.

2.2

a) Her bør kandidaten som minimum trekke inn utfordringer ved å gjøre risikovurderinger (ikke transparent) samt mulige utfordringer ved hendelseshåndtering. I tillegg bør det berøres hvordan man kan få utfordringer nå en leverandør ikke kan oppfylle sine forpliktelser
b) Her bør kandidaten som minimum trekke inn avtaler (spesielt *databehandleravtale)* og at man må opprettholde kompetanse for å kvalitetssikre/overvåke/risikovurdere internt

2.3

a) Her bør kandidaten som minimum forklare at sikkerhetskultur innebærer implisitte og eksplisitte føringer for holdninger, kunnskap, verdier samt generelt hvordan personalet håndterer sikkerhetshendelser. Det bør skilles fra personellsikkerhet som er regler og rutiner for ansettelse, ansettelsesforhold og avslutning av ansettelsesforhold. Det bør knyttes opp mot informasjonssikkerhetspolicy som en form for målsetningen og begrunnelse for sikkerhetskulturen. Sikkerhetskultur bør også skilles fra IT-reglement, som er konkrete regler man må følge uten å ha holdninger og kunnskap innen sikkerhet. Studenten forventes å definere sikkerhetskultur som noe mer enn regler, da den ansatte også vil være i stand til å håndtere hendelser det ikke finnes regler for.

b) Her bør kandidaten berøre rutiner for og håndtering av varsling, hvordan personlige feil håndteres, opplæring/ kompetanseheving, fokusering, prioritering og tydeliggjøring fra ledelsen