

# i Introduksjon

## EKSAMEN

**Emnekode:** ITF15015

**Emnenavn:** Innføring i datasikkerhet

**Dato:** 15/05-2020

**Eksamenstid:** 09.00-13.00, 4 timer + 15 minutter til innlevering i Inspira

**Hjelpemidler:** I hovedsak skal oppgavesettet besvares ut i fra hva man selv kan. Hentes informasjon fra andre kilder **skal dette siteres**, og slik avskrift vil ikke telle like positivt som egenprodusert tekst/kunnskap. Samarbeid mellom eksamenskandidater eller hjelp fra andre personer er **ikke tillatt**, og blir ansett som fusk (dersom fusk blir bevist fører det til utestengelse fra studiet). Det vil bli utført ulike kontroller for å avdekke avskrift, samarbeid og hjelp.

**Faglærer:** Tom Heine Nätt

### **Om eksamensoppgaven:**

Oppgavesettet er inndelt i 3 oppgaver. Det er på hver del, og deloppgavene i del 2, angitt hvor mye disse teller av totalen. **Karakter fastsettes dog på basis av en helhetsvurdering av besvarelsen.**

Gjør dine egne forutsetninger dersom du mener noe er uklart.

**Lykke til!**

**Sensurfrist:** 08/06-2020

Karakterene er tilgjengelige for studenter på Studentweb.

# 1 Oppgave 1 - 35 %

## Oppgave 1.1

Du får i oppgave, basert på det du har lært i emnet, å lage 10 sikkerhetsråd for privatpersoner med "*normalt kompetansenivå og normalt bruk av digitale tjenester og utstyr*". Det viktigste rådet bør stå først, og det "minst viktige" til sist. Hvilke råd vil du lage? Dersom du føler behov for det, må du gjerne spesifisere hva du legger i normalt kompetansenivå og normalt bruk.

## Oppgave 1.2

For hvert råd, forklar hvorfor nettopp dette rådet er tatt med og hva det kan bidra til å forhindre.

## Oppgave 1.3

Hvordan vil listen med råd fra oppgave 1.1 se ut dersom den heller skal utarbeides for ansatte i en bedrift? Du kan her ta utgangspunkt i antatt kompetansenivå og bruksmønstre til ansatte i studieadministrasjonen på HiØ (studieplaner, studieveiledning, eksamenskontor med mer). Du skal IKKE spesialtilpasse rådernes utforming til ansatte på HiØ, men tenke på "den typen arbeid og arbeidstakere" i mange ulike bedrifter. Du kan her legge til, fjerne, omformulere og endre rekkefølge på rådene fra oppgave 1.1. Dersom du føler behov for det, må du gjerne spesifisere hva du legger i kompetansenivå og bruksmønstre for ansatte tilsvarende de i studieadministrasjonen på HIØ.

## Oppgave 1.4

Begrunn endringene du har gjort fra oppgave 1.1 til 1.3

*Skill oppgave 1.1, 1.2, 1.3 og 1.4 slik at oppgave 1.1 og 1.3 kun er 10 nummererte råd. Du kan henvise til "rådnnummeret" i oppgave 1.2 og 1.4. Sørg for at oppgave 1.1 og 1.3 begge viser den komplette listen.*

*På en slik oppgave finnes det selvsagt ingen "fasit". Du vil bli vurdert på hvordan rådene viser at du behersker pensum, og hvor godt du argumenterer for hvert råd.*

## 2 Oppgave 2 - 55 %

Den private barnehagen Strupeberget AS har fått flere bekymringsmeldinger fra foreldre som lurer på om barnas opplysninger blir sikkert lagret og håndtert.

Barnehagen har 90 barn, tre avdelinger og 30 ansatte.

Til sammen har de tre bærbare maskiner (én plassert på hver avdeling) og én stasjonær maskin plassert hos styrer. I tillegg får ansatte en kompensasjon på 500 kr/år for å benytte sine egne mobiler i arbeidshverdagen. Barnehagen har også 8 digitale kompaktkameraer som går litt på rundgang i avdelingene. Disse benyttes til å ta bilder av barna som gis til foreldre (deles gjennom barnehagens IT-system, mer om det snart) og som henges opp på avdelingen. I tillegg benyttes kameraene for å dokumentere mer kritiske situasjoner og barnas utvikling, da man ikke ønsker at ansattes mobiler skal benyttes til dette. Hele barnehagen deler en nyinnkjøpt multifunksjonsprinter som er plassert i gangen, der alle avdelinger har lett tilgang når de skal skrive ut eller scanne noe.

Alle digitale enheter i barnehagen går på samme trådløse nett. Dette er WPA2-kryptert med en felles nøkkel/passord. Nettet benyttes også av enkelte foreldre som har fått passordet til bruk på foreldremøter osv.

I barnehagen kjøres det et web-basert IT-system som barnehagen selv har fått utviklet av en konsulent i 2013. I dette systemet lagres bilder, navn, fødselsnummer, allergier, religion, familiesituasjon (slik som søsken, skilte foreldre, personer som har lov til å hente barnet osv.), sykdommer, kontaktinformasjon til foreldre, pedagogiske/fysiologiske observasjoner av barnet og bekymringsmeldinger til barnevernet. I tillegg lagres informasjon om levering/henting/sykdom/fravær for barna hver dag.

Informasjonen fra IT-systemet lagres fysisk på den stasjonære kontormaskinen til styrer, der også serverdelen av dette systemet kjører. Her tas det backup en gang pr. dag til en ekstern harddisk som låses ned i skrivebordsskuffen. IT-systemet kan benyttes fra de bærbare maskinene, men også fra de ansattes mobiler.

For enkelhet skyld har alle ansatte på hver avdeling det samme brukernavnet/passordet til systemet, slik at man logger inn som "avdeling" og ikke person. Opplysninger om barnet som ikke krever daglig oppdatering (alt **annet** enn levert/hentet/syk/fravær og bilder) er det kun mulig å legge inn via maskinen som står på styrers kontor. I utgangspunktet var tanken at styrer skulle legge inn dette, men i dag gjør også de ansatte det selv da styrer ikke alltid er til stede når informasjonen skal registreres. All informasjon i systemet er derimot lesbart av alle ansatte på alle enheter. Lister med allergier, sykdom og religion har i det siste blitt skrevet ut, da ansatte i ett tilfelle glemte å sjekke IT-systemet, og barn fikk mat de ikke skulle ha.

En nedskalert portal er tilgjengelig for foreldre. Foreldrepar (mor+far) har en brukerkonto (brukernavn/passord) som benyttes for å få tilgang til informasjon om sitt barn i systemet. Når en foreldre logger inn vil man kunne se all registrert informasjon om barnet, med unntak av bekymringsmeldinger til barnevernet og

observasjoner av barnet. Spesielt bilder tatt av barnet er populært å hente ut via denne portalen. I tillegg vil man få oversikt over alle registreringer om levering og henting. Det er også mulig å selv registrere sykdom og fravær. Brukernavn og passord til foreldrenes brukerkonto gis i form av en "lapp i hylla" når barna starter i barnehagen.

Dersom det er mer generell informasjon du synes mangler i caset, som ikke dekkes av "sjekkene" i oppgave 2.1, så lage en punktliste med egne forutsetninger samlet først i besvarelsen av oppgaven.

### **Oppgave 2.1 – 30 %**

Identifiser ulike problemer barnehagen har med sikkerheten, og hva som kan gjøres av tiltak. Du vil selvsagt ikke rekke alt, men fokuser på å vise bredden i hva du kan (alt fra teknisk til "menneskelig" sikkerhet). Der ting ikke er beskrevet detaljert nok i caset skal du skrive hva du ville sjekket (intervjuer, kontroller, spørreundersøkelser, observasjoner osv.), og så hva ulike funn i praksis vil bety. I besvarelsen skal du skille de ulike sikkerhetsproblemene tydelig fra hverandre (for eksempel med beskrivende overskrifter).

### **Oppgave 2.2 – 12,5 %**

Gjør en enkel, men formell, risiko og sårbarhetsanalyse der du tar for deg **tre** av sikkerhetshendelsene/problemene fra oppgave 2.1. De opplysningene du mangler for å gjøre analysen kan du gjøre en kvalifisert gjetting på...

### **Oppgave 2.3 – 12,5 %**

Diskuter hva innføringen av GDPR kan bety for barnehagen. Både konkret på mangler og tiltak som bør gjøres, men også mer generelt på sikkerhetsarbeid og prioriteringer.

### 3 Oppgave 3 - 10 %

Med et eget eksempel og egne ord, forklar hva CSRF/webtrojaner er. Du trenger ikke lage eksempelet med kode eller grafikk, kun forklare det som er nødvendig for å vise at du vet hva CSRF er.