Bacheloroppgave

NTNU
Norges teknisk-naturvitenskapelige universitet
Fakultet for informasjonsteknologi og elektroteknikk
Institutt for datateknologi og informatikk

Marte Marjorie Søgnen
Ragna Skjei

Koronapandemiens påvirkning på personlig datasikkerhet

En casestudie hos HelseIT

Bacheloroppgave i Digital forretningsutvikling

Mai 2021

NTNU
Kunnskap for en bedre verden

Marte Marjorie Søgnen
Ragna Skjei

Koronapandemiens påvirkning på personlig datasikkerhet

En casestudie hos HelseIT

Bacheloroppgave i Digital forretningsutvikling
Mai 2021

Norges teknisk-naturvitenskapelige universitet
Fakultet for informasjonsteknologi og elektroteknikk
Institutt for datateknologi og informatikk

NTNU

Kunnskap for en bedre verden

Forord

Denne bacheloroppgaven er et resultat av en treårig utdanning i Digital forretningsutvikling, ved Norges teknisk-naturvitenskaplige universitet i Trondheim. Oppgaven er skrevet ved Institutt for datateknologi og informatikk, våren 2021. Temaet datasikkerhet ble presentert for oss i studiets fjerde semester, i emnet *Informasjonssikkerhet og produktforvaltning*. Dette temaet synes vi var særlig interessant, og derfor noe vi ønsket å skrive oppgave om. I samarbeid med oppgavestiller kom vi til enighet om at dette temaet var noe virksomheten ville ha stor interesse av å undersøke. Sammen med casebedriften og vår veileder kom vi frem til at vi ønsket å se nærmere på virksomhetens sikkerhetsinstruks, og virkningene av denne. For oss var det viktig å skrive om et tema vi selv fant interessant, samtidig som det var av nytte for casebedriften.

Vi vil takke våre to kontaktpersoner i casebedriften for et lærerikt semester, funn av informanter og god veiledning gjennom våren. Samtidig vil vi takke de for godt engasjement og samarbeid. Vi vil også takke oppgavens informanter for deltagelse, og innsiktsfulle besvarelser og refleksjoner. Dette har vært til stor hjelp for å kunne gjennomføre vår bacheloroppgave.

Til slutt vil vi takke vår veileder, Torstein Elias Løland Hjelle, for svært gode tilbakemeldinger, samt engasjement, hjelp og støtte underveis i forskningsprosessen. Arbeidet med bacheloroppgaven har vært svært lærerikt, og vi har fått en dypere forståelse av hvor komplekst sikkerhetsarbeidet i en virksomhet er.

Trondheim, mai 2021

Sammendrag

Dagens trusselbilde mot norske virksomheter er i stadig endring, og det fremkommer kontinuerlig nye sårbarheter en må beskytte seg mot. Bedrifter må derfor opprettholde tilstrekkelig informasjonssikkerhet. Med informasjonssikkerhet menes sikring av måten en behandler en virksomhets informasjonsverdier, ved å ta vare på dens konfidensialitet, integritet og tilgjengelighet. For samfunnskritiske organisasjoner vil det være spesielt viktig å opprettholde tilstrekkelig datasikkerhet på et personlig nivå hos alle ansatte. En sikkerhetsinstruks presenterer de retningslinjene en må forholde seg til, og tar for seg de viktigste punktene en virksomhet anser som essensielt for å opprettholde god sikkerhet. Denne bør derfor være utarbeidet i takt med dagens endrede trusselbilde, men hvilken betydning har det dersom den ikke er det? Koronapandemien kom til Norge i mars 2020, og over natten ble store deler av Norges befolkning tvunget til å jobbe hjemmefra. Samtidig ble det registeret nye sårbarheter direkte rettet mot hjemmekontor og digital samhandling. Casebedriften oppgaven baserer seg på har samtidig gjennomgått en stor endringsprosess, og befinner seg nå i en transisjonsfase. Med denne oppgaven vil vi forsøke å besvare *hvordan en sikkerhetsinstruks kan påvirke en organisasjon i endring under koronapandemien?*

Denne oppgaven tar utgangspunkt i casestudie som forskningsdesign, hvor vi har brukt kvalitative data i form av semistrukturerte intervju som vårt datagrunnlag. Dette skal i oppgaven settes i sammenheng med relevant teori, for å kunne besvare oppgavens problemstilling. Det er også for å knytte teorien til en kontekst, samtidig som teorien underbygger våre resultater. Da vi samtidig har benyttet oss av en abduktiv tilnærming har vi dynamisk beveget oss mellom empiri og teori gjennom forskningsprosessen. Dette har medført at arbeidet med utvikling av problemstilling har vært en iterativ og kontinuerlig prosess. På bakgrunn av hjemmekontor og mangelfull opplæring, i sammenheng med virksomhetens nåværende sikkerhetsinstruks, risikerer casebedriften at nyansatte ikke blir en del av sikkerhetskulturen. Vår oppgave fremmer viktigheten av en tydelig og godt formulert instruks, og rapporten retter et søkelys mot at hjemmekontor kan ha vært negativt for sikkerhetskulturen til virksomheter med sensitiv informasjon i sine systemer.

Abstract

Today's threat to Norwegian companies is constantly changing, and new vulnerabilities are continually emerging. Organizations should protect themself from these vulnerabilities and maintain adequate information security. Information security means securing the way one treats a company's information values by taken care of its confidentiality, integrity, and availability. For socially critical organizations, it will be essential to maintain adequate data security on a personal level for all employees. A security instruction presents guidelines one must adhere to and addresses the most critical subjects a business considers essential for maintaining sufficient data security. Organizations should develop security instruction in line with today's changing threat picture, but what significance does it have if it's not? The coronavirus pandemic came to Norway in March 2020, and overnight, Norway's population was forced to work from home. Simultaneous new vulnerabilities were registered directly aimed at home offices and digital interaction. Our assignment's case organization also had a significant change process and is now in a transition phase. With this assignment, we will try to answer *how a security instruction can affect an organization in change during the coronavirus pandemic?*

This thesis is based on a case study as a research design, where we have used qualitative data in the form of semi-structured interviews as our data sources. The data will be put in context with relevant theory to answer the thesis question and support our results. As we have also used an abductive approach, we have dynamically moved empiricism and theory through the research process. The work of developing the thesis problem has therefore been an iterative and continuous process. Our assignment shows that the case organizations' security instruction may have a considerable impact on the organization's security culture. New employees do not become part of the culture due to home offices and inadequate training. It emphasizes the importance of clear and well-formulated instructions. The thesis also focuses on the fact that home offices may have been harmful to the security culture of companies with sensitive information in their systems.

Innholdsfortegnelse

Figurer

Tabeller

Vedlegg

1 Introduksjon

Denne oppgaven tar utgangspunkt i undersøkelser gjennomført i en virksomhet hvor det stilles store krav til informasjonssikkerhet. Casebedriften ønsker å bli anonymisert, og i denne oppgaven vil vi derfor kalle organisasjonen HelseIT. HelseIT har ansvar for å drifte, forvalte og utvikle nasjonale helseløsninger og infrastruktur. Begrepet informasjonssikkerhet omhandler hvordan man sikrer behandlingen av analog og digital informasjon (Nätt, 2020). Med dette menes å ivareta informasjonens konfidensialitet, integritet og tilgjengelighet, som er selve fundamentet innen informasjonssikkerhet. Informasjon er konfidensiell når den skjules for uautoriserte personer eller systemer. Informasjon har integritet når den er komplett, og ikke korrupt. Med dette menes at informasjonen ikke har noe verdi dersom brukeren ikke kan stole på at den er riktig. Tilgjengelighet handler om at en kan få tilgang til informasjon uten store hindringer (Bergsjø & Windvik, 2018, s. 25). Informasjon blir behandlet i et samspill mellom teknologi, mennesker og prosesser. Det er dermed ikke kun det tekniske som må være sikkert for å opprettholde god informasjonssikkerhet. I tillegg til sikring av IKT-systemer og komponenter, er det nødvendig med sikre arbeidsprosesser, samt ha ansatte med god kompetanse som kan bidra til en sikkerhetskultur (Direktoratet for forvaltning og økonomistyring, 2020). For å kunne opprettholde tilstrekkelig informasjonssikkerhet i en virksomhet blir derfor personellsikkerhet viktig. Med personellsikkerhet menes det at alle involverte er bevisst rundt sine ansvarsområder, samt egnet til rollen en har i en virksomhet (Nettvett, 2020). Dette for å sikre en lav sikkerhetsrisiko (Nasjonal sikkerhetsmyndighet, 2019).

Det er mange ulike trusler rettet mot virksomheter i dagens samfunn. En trussel er en tilsiktet uønsket handling (Bergsjø & Windvik, 2018, s. 18). Koronapandemien har medført at store deler av Norges befolkning sitter på hjemmekontor, noe som kommer frem i PSTs nasjonale trusselvurdering for første kvartal av 2021. I rapporten fremkommer det at «*Etterretningstjenester vil utnytte reduserte digitale sikkerhetsmekanismer i hjemmekontorløsninger. Slike løsninger øker sannsynligheten for at nettverksoperasjoner vil lykkes*» (Politiets sikkerhetstjeneste, 2021, s. 14). Koronapandemien har medført nye sårbarheter for virksomheter fordi fjerntilgang og hjemmekontor har skapt et stort behov for nye digitale løsninger. Sårbarheter som avlytting, inntrenging og angrep via internett blir presentert (Nasjonal

sikkerhetsmyndighet, 2021). Politiet sier virksomheter i koronapandemien i større grad blir utsatt for direktørsvindel, som blant annet er knyttet til smitteforebygging (Politidirektoratet, 2021, s. 24). Direktørsvindel er når en aktør utgir seg for å være sjef eller leder i en bedrift. Formålet med denne type svindel er å få økonomimedarbeidere til å overføre penger til en annen konto. Typisk for dette er å sende falsk faktura via e-post, gjerne med påskudd om hastende betaling (Bergsjø & Windvik, 2018, s. 49). At de ansatte er bevisst over hvilke sårbarheter og trusler som finnes er derfor vesentlig for å gjennomføre arbeidet så sikkert som mulig.

1.1 Om Casebedriften

HelseIT har kontorer lokalisert i Trondheim, Oslo, Bergen og på Svalbard, men våre undersøkelser er basert på informasjon fra virksomhetens hovedkontor i Trondheim. Virksomheten besto i 2018 kun av 373 ansatte, men har de siste årene opplevd en kraftig vekst, og består nå av omtrent 700 ansatte. De befinner seg nå i en tidlig modningsfase etter en sammenslåing av to selskaper. Dette har ført til store endringer fra år 2020 da de tok over 200 nye ansatte. Endringene omhandler i stor grad omorganisering, og for sikkerhetsavdelingen har de innført et nytt styringssystem for informasjonssikkerhet, forkortet ISMS. Et ISMS er et system som sier noe om hvordan ledelsen håndterer og kontrollerer datasikkerhet innad i en organisasjon (Bergsjø & Windvik, 2018, s. 27). I tillegg er HelseIT blitt en hierarkisk sikkerhetsorganisasjon som gir klare ansvarsområder for sikkerhetsdirektøren og sikkerhetslederne.

HelseIT har på bakgrunn av rask vekst vært nødt til å endre sine opplæringsrutiner i forhold til personlig sikkerhet, da det ikke lenger er mulighet for gjennomføring av organisert fysisk opplæring. Tidligere har sikkerhetsopplæringsleder hatt ansvar for dette, men dette er vanskelig å gjennomføre da rekrutteringen i dag skjer svært raskt. I tillegg til nye opplæringsrutiner er endring av virksomhetens sikkerhetsinstruks nødvendig for samsvar mellom det som kommuniseres til de ansatte, og det som står nedskrevet i dokumentet. Arbeidet med ny sikkerhetsinstruks er foreløpig satt på vent, og en valgte i stedet å prioritere virksomhetens ISMS grunnet sammenslåingen. Sikkerhetsinstruksen er derfor vært uendret gjennom en lengre periode. Dette resulterer i en instruks som ikke gjenspeiler virksomhetens budskap hva gjelder sikkerhetsopplæring, og de basiskrav som stilles til de ansattes sikkerhetsrutiner.

Virksomheten befinner seg nå i en transisjonsfase der de må tenke nytt når det gjelder opplæring og sikkerhet. En må bruke nye virkemidler for å holde oversikt over hvilke av de ansatte som har fått kurs, og hvordan kurset ble gjennomført. Koronapandemien har på mange måter gjort dette arbeidet vanskelig, da både ansatte og ledere sitter på hjemmekontor.

1.2 Presentasjon av oppgavens problemstilling

For at HelseIT skal være så sikre som mulig i sitt sikkerhetsarbeid er det nødvendig at de ansatte er klar over hvilke sårbarheter en bør sikre seg mot. På bakgrunn av de store endringene virksomheten har vært igjennom det siste året, samt koronapandemien, vil vi undersøke betydningen av dagens sikkerhetsinstruks. Da koronapandemien brøt ut i mars 2020 var hjemmekontor sett på som en midlertidig løsning. En så ikke for seg at en over et år senere fortsatt jobbet hjemmefra. Under pandemien er sikkerhetsopplæringen i HelseIT blitt mangelfull, og på hjemmekontor kan det bli vanskelig å ta del i virksomhetens kultur. Dette er hovedårsaken til at vi velger å inkludere koronapandemien i problemstillingen, da dette er en betydelig faktor for hvorfor sikkerhetsopplæringen er blitt svekket. Etter koronapandemien kom, er sikkerhetsinstruksen nærmest den eneste formen for opplæring en nyansatt får. Vi vil i denne oppgaven se nærmere på hvordan sikkerhetsinstruksen påvirker virksomheten, hvor en både er i en avsluttende fase av endring, samtidig som en befinner seg i en pandemi. På bakgrunn av dette er det blitt formulert følgende problemstilling:

«Hvordan kan en sikkerhetsinstruks påvirke en organisasjon i endring under koronapandemien?»

1.3 Oppgavens avgrensninger og oppbygning

Vår oppgave tar utgangspunkt i sikkerhetsinstruksen til vår casebedrift. En sikkerhetsinstruks vil være forskjellig fra virksomhet til virksomhet, og våre resultater og funn er kun basert på denne organisasjonen. Detaljene i denne oppgaven er derfor spesifikt for HelseIT, men det overordnede vil kunne gjelde andre samfunnskritiske virksomheter som Forsvaret, politiet og Tolletaten. Det vil kunne være viktig for andre virksomheter å undersøke hvordan koronapandemien har påvirket ansattes

datasikkerhet, og kanskje spesielt for nyansatte. Dette fordi hjemmekontor skulle være en midlertidig løsning, men som på mange måter er kommet for å bli. Ved å belyse dette temaet i vår oppgave, vil flere kunne sette inn tiltak for å lettere komme tilbake til normalsituasjon.

Oppgaven er delt inn i seks hovedkapitler, hvor det første kapittelet introduserer bakgrunnen for oppgaven, casebedriften og vår problemstilling. Videre presenteres all relevant teori som senere vil bli diskutert opp mot oppgavens problemstilling. I kapittel tre beskrives valg av metode og forskningsdesign, som setter rammene for forskningsprosessen. Våre funn blir presentert og analysert i kapittel fire, som sammen med teori vil bli diskutert opp mot problemstillingen i kapittel fem. Det avsluttende kapittelet baserer seg på teori, resultater og diskusjon, hvor vi presenterer vår konklusjon av problemstillingen.

2 Teorigrunnlag

I dette kapittelet presenterer vi relevant teorigrunnlag for oppgavens problemstilling. Kapittelet er delt inn i fem underkategorier: organisasjonskultur, holdninger og vaner, motivasjon, kommunikasjon, samt ledelse. Teorien vil bli benyttet i kapittel fem, hvor vi diskuterer resultater og teori opp mot hverandre. Dette vil være utgangspunktet for å kunne besvare vår problemstilling.

2.1 Organisasjonskultur

Kultur betyr å dyrke, eller å pleie, og omhandler tanke-, kommunikasjons- og atferdsmønstre hos mennesker (Schackt, 2019). Organisasjonskultur er mønstre som befinner seg blant ansatte innad i en virksomhet, og det er nødvendig å vite hva organisasjonskultur er for å forstå hvordan en virksomhet fungerer. Ifølge Cummings og Worley (2019) har fokus på organisasjonskultur i stor grad vokst fram de siste 30 årene. Forskere har derimot vært interessert i fenomenet allerede fra 1970-tallet, da en så at organisasjonskultur var en viktig faktor for bedrifters suksess (Jacobsen & Thorsvik, 2016). En organisasjons-kultur blir utviklet over tid, og innebærer et sett med felles verdier og normer for hvordan en opptrer på arbeidsplassen (Jacobsen & Thorsvik, 2016, s. 151). Verdier omhandler det menneskene i virksomheten strever etter, og ønsker å oppnå (Schackt, 2019). Normene er uskrevne regler som forteller hva som er akseptabelt i forhold til atferd. Som nyansatt vil en tilpasse seg organisasjonens normer, og om en ikke gjør det risikerer man å bli utsatt for sanksjoner (Busch, Dehlin, & Vanebo, 2010, s. 219).

Organisasjonskulturen kan i stor grad påvirkes av ledelsen, men gjenspeiles også gjennom organisasjonens omgivelser. Som leder kan en påvirke kulturen innad i organisasjonen ved selektiv rekruttering. Denne formen for rekruttering omhandler en kandidats kulturelle egnethet ved ansettelse. For å oppnå ønsket organisasjonskultur krever det også en godt planlagt sosialiseringsprosess. Gjennom denne prosessen danner den nyansatte seg en sosial identitet som en kan knytte opp mot andre personer i organisasjonen. En kan også se sammenhengen mellom nasjonal kultur og organisasjonskulturen i form av verdier og normer (Jacobsen & Thorsvik, 2016, s. 151). Organisasjonskultur spiller en rolle for hvordan ansatte opptrer på sin arbeidsplass. For

å få et nyansert og klart bilde over en virksomhets organisasjonskultur er det viktig å vite hva kultur i utgangspunktet innebærer. Dette er derfor viktig for enhver virksomhet.

2.1.1 Sikkerhetskultur

En virksomhets sikkerhetskultur befinner seg innad i organisasjonskulturen. En sikkerhetskultur er *«de verdier, holdninger, antakelser, normer og kunnskaper som mennesker bruker når de forholder seg til informasjonsverdier»* (Norsk senter for informasjonssikring, 2017, s. 16). Det handler derfor om hvordan mennesker forholder seg til informasjonsverdiene, samt hvordan en styrer sikkerheten i en virksomhet (Næringslivets Hovedorganisasjon, 2021). For å skape en god sikkerhetskultur må en som leder motivere sine ansatte til å utøve sine arbeidsprosesser på en måte som tilfredsstiller sikkerhetskravene. Ved å ha en god sikkerhetskultur vil medarbeiderne bidra til å opprettholde de sikkerhetstiltakene som er viktige for virksomheten (Nasjonal sikkerhetsmyndighet, s. 11). Spesielt i virksomheter hvor en må forholde seg til sensitive informasjonsverdier vil en god sikkerhetskultur være viktig. Dersom ansatte ikke forholder seg trygt til verdiene vil det kunne få store konsekvenser.

2.1.2 Digital kultur

Digital kultur kjennetegnes ofte av organisasjoner med stort fokus på eksperimentering, datadreven beslutningstaking og et engasjement for kunder og resultat. Det er fire hovedprinsipper ved digital kultur: påvirkning, hastighet, åpenhet og autonomi. Prinsippene handler i stor grad om at en som teknologiorganisasjon skal endre verden i stor grad gjennom kontinuerlig innovasjon. En legger stor vekt på iterative prosesser som øker hastigheten på eksempelvis beslutningstaking. Istedenfor å holde kunnskap for seg selv, oppfordres man til å dele denne med alle i organisasjonen for å skape engasjement og læring. En skal til slutt la de ansatte gjøre det som trengs i gitte situasjoner, heller enn å la de styres av struktur og regler (Eswaran, Soule, & George, 2019, s. 61).

Selv om innovasjon og hurtighet er sentralt, er det viktig å ta hensyn til samspillet mellom mennesket og teknologien. Hvis en endrer teknologien uten å ta hensyn til kulturen kan dette skape lavere effektivitet og dårligere kvalitet på arbeidsutførselen. Altså har allerede eksisterende teknologi, samt innføring av ny teknologi, stor betydning for relasjonen mellom de ansatte, samt organisasjonens arbeidsmiljø (Busch, Dehlin, &

Vanebo, 2010, s. 152). Digital kultur kan oppleves annerledes fra avdeling til avdeling. For noen vil det være lagt stor vekt på nøyaktighet og forsiktighet ved bruk av teknologi. For andre vil heller kreativiteten ved teknologien være sentral (Busch, Dehlin, & Vanebo, 2010, s. 225).

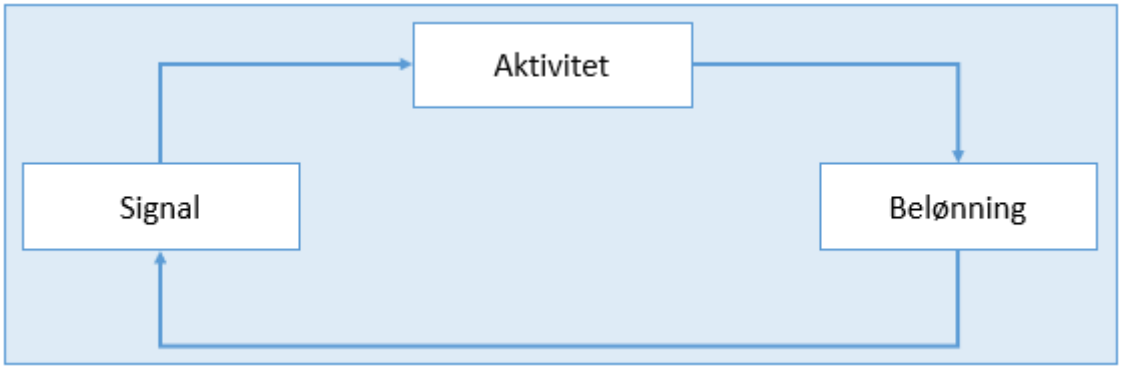
Under koronapandemien er det viktig å forstå hvordan hjemmekontor og bruk av digitale plattformer påvirker organisasjonskulturen. Ved å snakke med hverandre over plattformer som Slack, Skype og Microsoft Teams vil en virksomhets kultur være noe annerledes enn om en hadde vært i virksomhetens egne lokaler. En opplever ikke på samme måte den hverdagslige praten. Oppfatning av normer, holdninger og atferd hos andre ansatte kan på mange måter falle bort ved å prate med hverandre over digitale flater. En negativ påvirkning på kvaliteten av arbeidsutførselen, samt effektivitet kan i tillegg oppstå når de ansatte sitter på hjemmekontor. Dette fordi det meste av samarbeid foregår over samhandlingsplattformer. Digital kultur er derfor relevant for vår problemstilling.

2.2 Holdninger og vaner

Allerede i 1932 utarbeidet sosialpsykologen Rensis Likert Likerts-skalaen for å måle individers holdninger (Jamieson, 2007). Videre på 1950-tallet la forskere frem teorier om forholdet mellom holdninger og atferd. Den dag i dag er det fortsatt stor interesse for område da en ser at kunnskap om holdningsendring kan bidra til å redusere uønsket atferd (Svartdal, 2020). En holdning er en innlært impuls som resulterer i positive eller negative reaksjoner på en gitt situasjon eller et objekt (Selnes & Lanseng, 2014). En persons holdninger skapes gjennom opplevelser, kunnskap og erfaring. Holdningene læres over tid, og fører til en konsekvent adferd. Positive holdninger gjør en person interessert og åpen. Negative holdninger vil derimot føre til adferd som kan oppleves uinteressert og motvillig. Gjennom bevisstgjøring fra ledelsen og andre ansatte kan en persons holdninger på arbeidsplassen endres (Bostad, Røyert, & Paulsen, 2020). Holdninger er en svært viktig komponent når det kommer til læring. Dersom en har mestringstro, og selvtillit til eget arbeid, vil en ha en bedre forutsetning for å lære. Dette vil også øke motivasjonen for å legge inn den innsatsen som trengs for å lære (Lai, 2017). Det er relevant å ta for seg teori om holdninger da dette påvirker villighet til læring gjennom sikkerhetskurs, seminarer og andre tiltak satt i verk av ledelsen. Har man

ansatte med gode holdninger vil dette gjenspeiles i deres vaner og utførsel av arbeidsoppgaver. Med mindre gode holdninger kan dette potensielt føre til uheldige hendelser og sikkerhetsbrudd.

En vane er en del av en større, automatisert rutine som foregår utenfor vår oppmerksomhet. Det er derfor vanskelig å motstå en vane. Allikevel vil et slikt automatisert adferdsmønster øke ansattes kapasitet, da utførselen av arbeidsoppgaver går ofte på automatikk (Karahanna & Polites, 2012, s. 25). For å forstå kompleksiteten av en vane kan den beskrives ved hjelp av vanesirkelen som vist i figur 2.1 (Duhigg, 2016, s. 313).



Figur 2.1 – Vanesirkelen (Duhigg, 2016, s. 313)

Denne sirkelen tar utgangspunkt i gjennomføringen av en *aktivitet*, et *signal* som resulterer i utførsel av aktiviteten, samt en *belønning* for utført arbeid. Det å forstå de ansattes vanesirkel er et godt utgangspunkt dersom en vil endre en dårlig vane. For å gå i gang med endring av en vane bør en ta utgangspunkt i belønningen, da dette ofte er drivkraften for den ansattes atferd (Duhigg, 2016, s. 313). Dersom en gjør noe ofte nok, vil dette over tid omformes til en vane. De ansattes vaner henger i stor grad sammen med organisasjonskulturen. Dersom en skal klare å endre en organisasjonskultur er en avhengig av å kunne endre hver enkelt medarbeiders vaner (Einarsen & Martinsen, 2019, s. 421).

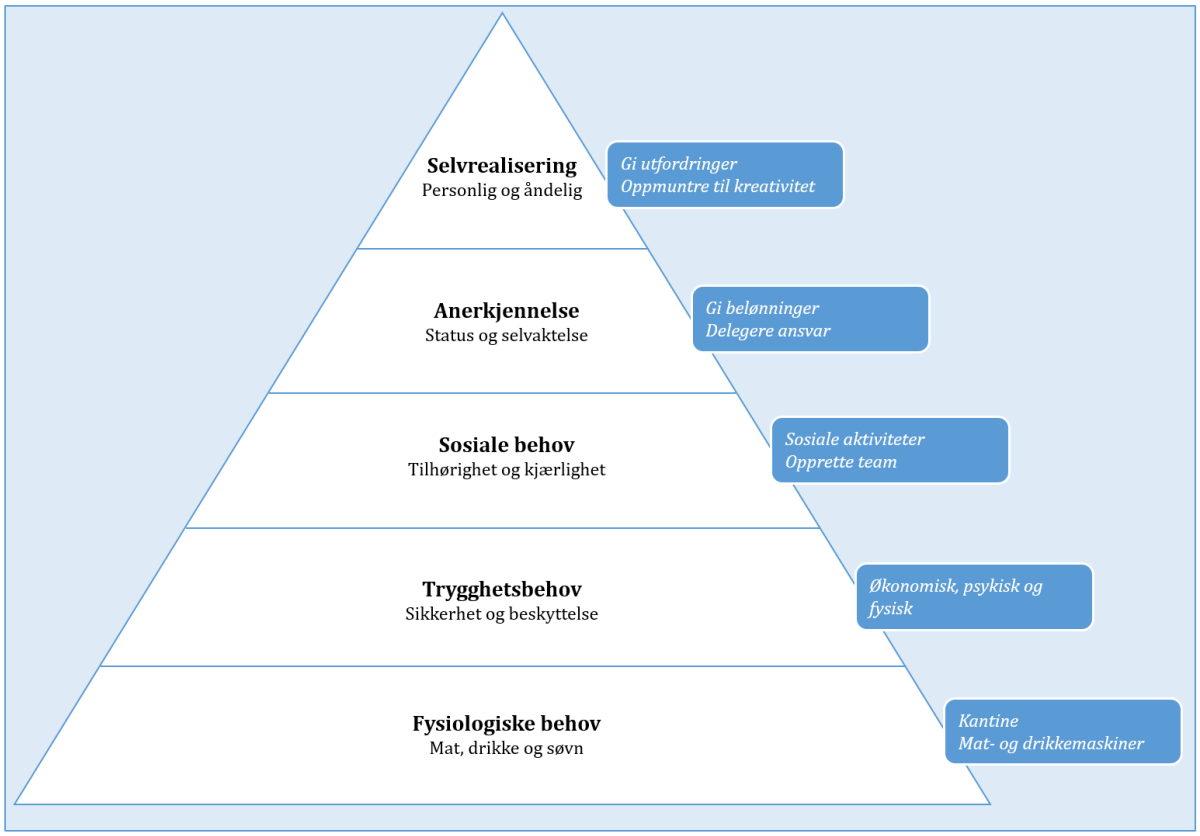
Vaner er relevant for ulike virksomheter da dette påvirker måten de ansatte utfører sine arbeidsoppgaver på. Gode vaner vil i mange tilfeller føre til økt sikkerhet. Dårlige vaner, som workarounds, kan derimot føre til små sikkerhetsbrudd som en gjerne vil unngå.

2.3 Motivasjon

Motivasjon omhandler alle de faktorene som styrer et individs atferd, og kommer fra det latinske ordet *movere*, som betyr «bevege» (Einarsen & Martinsen, 2019, s. 87;88). Geir og Astrid Kaufmann definerer motivasjon som *«de biologiske, psykologiske og sosiale faktorene som aktiverer, gir retning til og opprettholder atferd i ulike grader av intensitet for å oppnå et mål»* (Kaufmann & Kaufmann, 2014, s. 93). Det finnes forskjellige typer motivasjonsteorier, og det er vanlig å skille disse inn i behovsteorier, kognitive teorier, sosiale teorier og jobbkarakteristika-modeller. Behovsteoriene mener motivasjon oppstår dersom grunnleggende behov er tilfredsstilt, mens kognitive teorier sier at motivasjon oppstår ved forventet belønning. Sosiale teorier tar utgangspunkt i oppfattelsen om rettferdighet og likhet, mens jobbkarakteristika-modellen sier at det er visse nøkkelfaktorer knyttet til selve jobben som skaper motivasjon (Kaufmann & Kaufmann, 2014, s. 93). På bakgrunn av oppgavens problemstilling vil vi gå nærmere inn på en behovsteori, en kognitiv teori, samt en jobbkarakteristika-modell.

2.3.1 Maslows behovshierarki

Abraham Maslow presenterte allerede i 1943 det første utkastet til behovshierarkiet, og den ble i ettertid videreutviklet før hans død i 1970 (Mørch, 2020). Han mente at menneskelige behov var delt inn i fem nivå: fysiologiske behov, trygghetsbehov, sosiale behov, anerkjennelse og selvrealisering. Nivåene er blitt rangert systematisk, og teoriens hovedpoeng er at de laveste nivåene må tilfredsstilles på et visst minimum før en kan tilfredsstille de høyere nivåene (Bolman & Deal, 2018, s. 157). For å oppnå behovet for selvrealisering må de fire andre behovene være sikret. Nivåene blir igjen kategorisert i to hovedtyper: *mangelbehov* og *vekstbehov* (Einarsen & Martinsen, 2019, s. 89). Mangelbehovene tilsvarer de tre nederste nivåene i hierarkiet, mens vekstbehovene tilsvarer de to høyeste nivåene. En kan ikke oppnå personlig vekst dersom mangelbehovene ikke er tilfredsstilt (Kaufmann & Kaufmann, 2014, s. 95).



Figur 2.2 – Maslows behovshierarki, vår tolkning

Behovshierarkiet er illustrert i figur 2.2. Figuren viser de fem nivåene, og hvilke behov som bør dekkes. Til høyre presenteres det noen tiltak en kan gjøre for å tilfredsstille behovene på hvert nivå.

På det nederste nivået finner man de *fysiologiske behovene*, og er de grunnleggende behovene et menneske har for å overleve. Dette innebærer mat, drikke og søvn, men også en lønn som kan dekke disse behovene (Kaufmann & Kaufmann, 2014, s. 94). *Trygghetsbehov* blir også betegnet som et grunnleggende behov, og omhandler både økonomisk, psykisk og fysisk trygget. Sikkerhet i arbeidshverdagen, hvor en opplever stabilitet og forutsigbarhet vil være med å dekke dette behovet (Einarsen & Martinsen, 2019, s. 89). *Sosiale behov* er det siste grunnleggende behovet i teorien. Ansatte trenger et godt sosialt miljø, og positive omgivelser som tilbyr støtte. Deltagelse og samarbeid vil være elementer som kan dekke slike behov. Det fjerde nivået, behov for *anerkjennelse*, er det første stadiet en vil kunne oppnå motivasjon og vekst. Maslow mener et individ som befinner seg på dette nivået ikke vil fokusere mot de underliggende nivåene, men heller se mulighetene for vekst og videreutvikling. Annerkjennelse av arbeidet som gjøres er i stor grad med på å tilfredsstille behovet. Det siste, og høyeste, nivået er behovet for

selvrealisering. Her mener Maslow at motivasjon vil oppnås i høyeste grad. Et menneske som befinner seg på dette stadiet vil ha stor ytelse til å utvikle seg selv, samt å realisere sitt eget potensiale (Kaufmann & Kaufmann, 2014, s. 95).

Maslows behovshierarki er fra 1950-årene, og er den eldste og mest innflytelsesrike behovsteorien (Bolman & Deal, 2018, s. 156). Det er dog vanskelig å finne forskning som støtter teoriens troverdighet (Kaufmann & Kaufmann, 2014, s. 96). Det er ingenting som støtter at menneskelige behov er inndelt i et slikt hierarki med fem kategorier, og at et visst antall behov må være tilfredsstilt før en kan oppnå vekst. Forskning viser derimot at skillet mellom mangelbehov og vekstbehov er mer gyldig (Einarsen & Martinsen, 2019, s. 90). Dette gjør teorien til et godt ledelsesverktøy, og store selskaper som FedEx og Airbnb har med dette utviklet svært suksessrike filosofier innen ledelse (Bolman & Deal, 2018, s. 158). Dette er hovedårsaken til at vi ser på denne teorien som nyttig for vår problemstilling.

2.3.2 Kognitiv forventningsteori

Victor Vroom (1994), originalt publisert i 1964, var den første til å foreslå den kognitive forventningsteorien. Teorien sier at motivasjon og vilje til å yte vil oppstå, gitt at det eksisterer en forventning om belønning. Forventningsteorien omhandler begrepene valens, forventning og instrumentalitet (Ramlall, 2004, s. 56). Med *valens* menes styrken i forventet belønning. Den belønningen en får etter et resultat må være noe en ønsker seg. Dette vil være individuelt fra menneske til menneske, og det finnes derfor ingen fasit på hva en god belønning er (Einarsen & Martinsen, 2019, s. 96). *Forventning* er den viten om at det forekommer en belønning dersom en oppnår et bestemt resultat. For at et menneske skal yte en god innsats, må forventningen om en belønning være til stede. *Instrumentalitet* er den troen om at ønsket belønning vil forekomme ved et gitt resultat. Teorien sier at alle begrepene henger sterkt sammen, og at motivasjon er produktet av valens, forventning og instrumentalitet. Det betyr at dersom to verdier er høye, mens én verdi er på null, vil en ikke oppnå motivasjon. Sammenhengen mellom begrepene er illustrert i form av en motivasjonsformel, vist i figur 2.3 (Kaufmann & Kaufmann, 2014, s. 98).

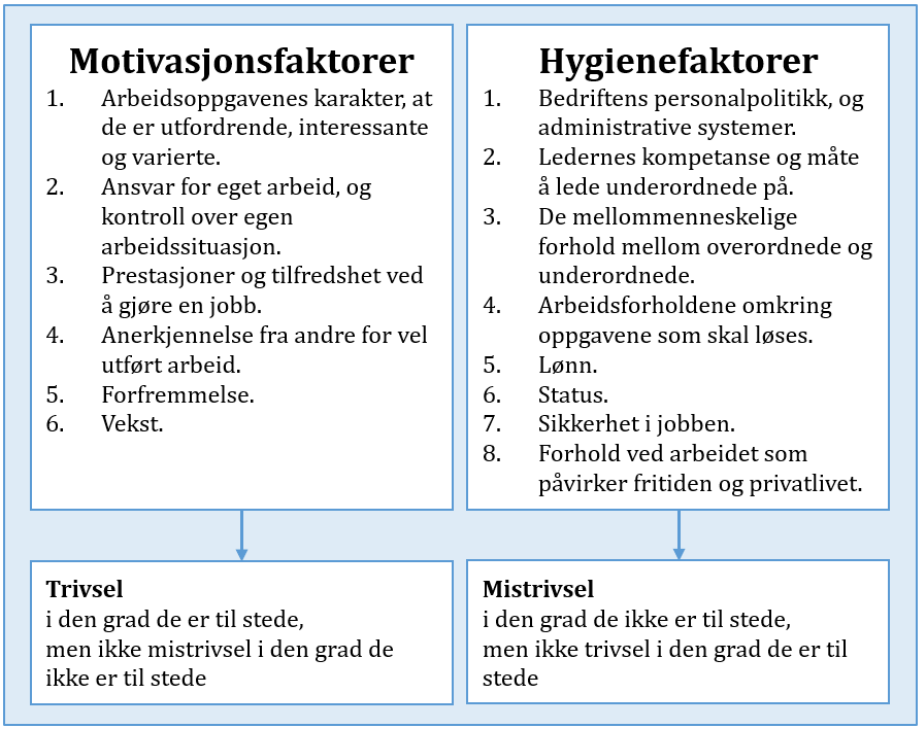
$$Motivasjon = valens * forventning * instrumentalitet$$

Figur 2.3 – Motivasjonsformelen, inspirert av (Kaufmann & Kaufmann, 2014, s. 98)

Forskning sier at store deler av forventningsteorien er troverdig, men at det er et multiplikativt forhold mellom begrepene er man i tvil om (Kaufmann & Kaufmann, 2014, s. 99). Det er også usikkerhet rundt hva begrepene betyr, og hvordan de skal kunne måles. Forskere mener allikevel det finnes en sammenheng mellom begrepene valens, forventning og instrumentalitet (Einarsen & Martinsen, 2019, s. 96). Vi ser derfor på deler av denne teorien som nyttig når en diskuterer motivasjon. For å skape motivasjon i en organisasjon kan det være hensiktsmessig å ta hensyn til de tre begrepene, og forsøke å gjøre verdien av disse så høye som mulig.

2.3.3 Herzbergs tofaktorteori

Jobbkarakteristika handler om at visse nøkkelfaktorer er med på å skape motivasjon. Disse faktorene er henholdsvis variasjon, ansvar og betydning. Med variasjon menes rotering av arbeidsoppgaver, hvor en benytter ulike ferdigheter. Ansvar handler om å ha eierskap til det en utfører, og betydning omhandler arbeidsoppgavenes viktighet (Kaufmann & Kaufmann, 2014, s. 111;112). Frederick Herzbergs tofaktorteori *«handler om hva som påvirker motivasjon, tilfredshet og misnøye hos ansatte»* (Sagberg, Frederick Herzberg, 2020). Herzberg kartla faktorer som førte til både trivsel og mistrivsel på arbeidsplassen, og registrerte at disse var forskjellige. Han kom derfor opp med et sett motivasjonsfaktorer og hygienefaktorer. Motivasjonsfaktorer er det som skaper trivsel på en arbeidsplass dersom de er til stede, men de vil ikke skape mistrivsel dersom de ikke finnes. Hygienefaktorene er de som skaper mistrivsel dersom de ikke er til stede, men som ikke vil skape trivsel dersom de eksisterer. Herzberg oppdaget derfor at begrepene trivsel og mistrivsel ikke er direkte motsetninger, fordi faktorene er forskjellig (Jacobsen & Thorsvik, 2016, s. 261).



Figur 2.4 – Herzbergs tofaktorteori (Jacobsen & Thorsvik, 2016, s. 261)

Figur 2.4 viser at faktorene for motivasjon omhandler anerkjennelse, ansvar og selve arbeidsoppgavene. Dette er såkalte indre sider ved jobben (Einarsen & Martinsen, 2019, s. 126), og nivåene ligger høyt opp i Maslows behovspyramide. Disse faktorene fremmer jobbtilfredshet dersom de er til stede. Hygienefaktorene innebærer lønn, sosiale forhold og trygghet, som handler om de ytre sidene ved en jobb (Einarsen & Martinsen, 2019, s. 126). Disse nivåene tilsvarer de lavere nivåene i Maslows behovspyramide og en ansatt vil oppleve mistrivsel dersom faktorene ikke er til stede.

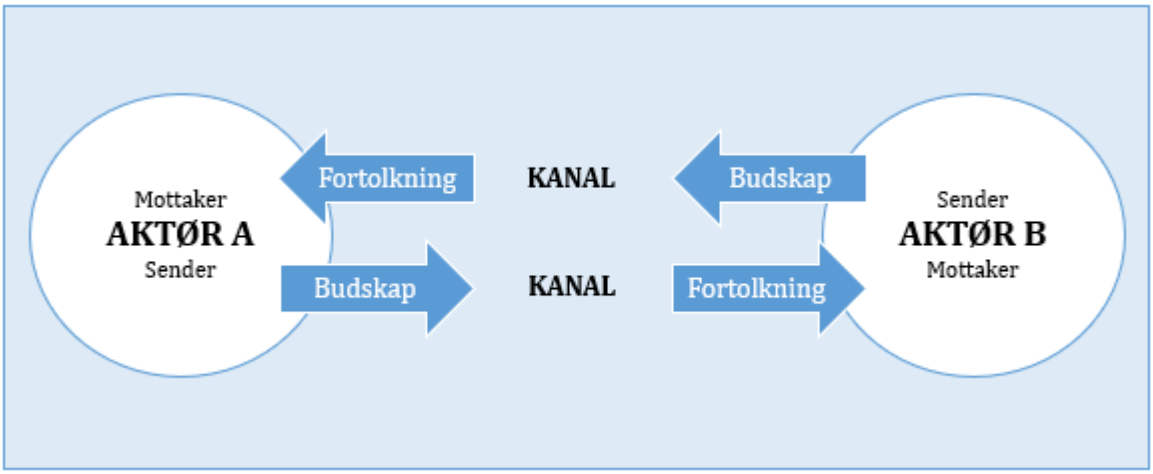
Slik som de tidligere motivasjonsteoriene har også tofaktorteorien blitt kritisert. Teorien har lite forskningsfunn, men en gjør seg allikevel noen bemerkninger som kan støtte teorien. Einarsen og Martinsen (2019, s. 126) skriver at det er *«vanskelig å forestille seg at spennende arbeidsoppgaver kan gjøre en arbeidstaker tilfreds med jobben dersom han mobbes dagen lang»*. Dette tyder på at Herzberg, til tross for kritikk, er inne på noe vesentlig når det kommer til trivsel og mistrivsel på arbeidsplassen. Samtidig viser det at motivasjonsfaktorene og hygienefaktorene ikke nødvendigvis veier like mye. Eksempelet viser at mistrivsel i større grad blir vektlagt, selv om faktorer for trivsel også er til stede. Denne teorien vil derfor være relevant for enhver virksomhet, for å bedre trivselen på arbeidsplassen.

2.4 Kommunikasjon

Begrepet kommunikasjon stammer fra det latinske ordet «*communicare*», som betyr å dele noe (Einarsen & Martinsen, 2019, s. 287). Ved å kommunisere bruker man språk for å formidle informasjon og ideer. En person som ønsker å kommunisere har et mål om å gjøre seg forstått for mottakeren (Allott, 2019). Informasjon, assosiasjoner, ideer, holdninger og følelser påvirker måten en person tolker det som kommuniseres. Men mye av kommunikasjonen mellom to eller flere mennesker er ikke-verbal. Altså kommer den fram gjennom kroppsspråk, stemmebruk og andre ikke-verbale signaler. Kommunikasjon er en dynamisk prosess der innholdet og dens formidler endres hele tiden (Sætre, 2009, s. 43). Teori om kommunikasjon er relevant for enhver virksomhet da gode kommunikasjonsferdigheter fra ledelsen har innvirkning på hvordan ansatte oppfatter norm, prosedyrer og retningslinjer. Mangelfull eller dårlig kommunikasjon kan føre til misforståelser og feil oppfatning av lederens budskap.

2.4.1 Kommunikasjonsprosessen

En kommunikasjonsprosess (figur 2.5) består av en sender som vil formidle sitt budskap, og en mottaker som mottar og tolker informasjonen som er gitt (Jacobsen & Thorsvik, 2016, s. 280). Sender må først formulere og utrykke det budskapet som ønskes formidlet. Dette innebærer valg av verbale og ikke-verbale signaler. Sender må videre velge hvilken kanal han eller hun skal bruke for å formidle informasjonen. Her kan valget stå mellom å formidle seg skriftlig eller muntlig, samt om en skal bruke kanaler som oppfattes formell eller uformell. Mottakeren fortolker budskapet for å gjøre seg opp en mening om hva senderen prøver å formidle. Her kan det oppstå kommunikasjonsproblemer, da en eksempelvis misforstår det sender prøver å formidle. Det siste leddet i prosessen er tilbakemelding. Altså gir mottaker svar til senderen av informasjonen etter sin fortolkning av budskapet (Busch, Dehlin, & Vanebo, 2010, s. 388).



Figur 2.5 – Kommunikasjonsprosessen (Jacobsen & Thorsvik, 2016, s. 281)

I figur 2.5 er stegene i kommunikasjonsprosessen illustrert. Her ser en tydelig hvilken rolle de ulike aktørene har når de kommuniserer med hverandre. Samt hvordan kanalen en velger kan påvirke mottakers fortolkning av budskapet.

Effektiv kommunikasjon kommer frem ved en felles forståelse mellom sender og mottaker. For å kunne oppnå dette må sender bruke et språk som mottaker forstår. Budskapet må i tillegg sendes gjennom en kanal som brukes og er forstått av mottaker, og må gis på en slik måte at det vil bli lagt merke til (Goodman & Truss, 2006, s. 218). Hvis en skal kommunisere noe av stor viktighet er det nyttig å gjenta budskapet ofte, gjerne gjennom ulike kanaler. Disse kanalene kan variere mellom ansikt- til- ansikt kommunikasjon, elektroniske kanaler, sosiale medier og informasjon på utskrift (Beatty, 2015, s. 13). Kommunikasjonsprosessen kan bidra til å skape god kommunikasjon i ulike virksomheter. Når bedrifter gjennomgår større endringer, kan det være aktuelt å forbedre sin kommunikasjonsprosess innad i virksomheten så den stemmer overens med de endringer som blir foretatt.

2.4.2 Elektroniske kanaler

Informasjons – og kommunikasjonsteknologi har på mange måter endret hvordan ansatte og ledere kommuniserer med hverandre innad i en virksomhet (Sætre, 2009, s. 21). Nye, elektroniske kommunikasjonskanaler som e-post, chat, samt video- og telefonkonferanser gir oss muligheten til å være uavhengig av tid og rom. Dette er på mange måter en positiv organisatorisk utvikling, da en eksempelvis kan dele informasjon raskt til flere personer samtidig. Allikevel gir det de ansatte mulighet til å være selektiv i

forhold til hvilken informasjon man velger å ta til seg. Ved bruk av elektroniske kanaler er det i mange tilfeller geografisk avstand mellom sender og mottaker. Fysisk avstand trekkes dermed frem som en mulig kommunikasjonsbarriere (Karlsen, 2018, s. 255). Dette, i tillegg til det faktum at elektroniske kanaler i noen sammenhenger mangler evnen til å formidle rik informasjon, gir disse kanalene rom for feiltolkning (Jacobsen & Thorsvik, 2016, s. 287).

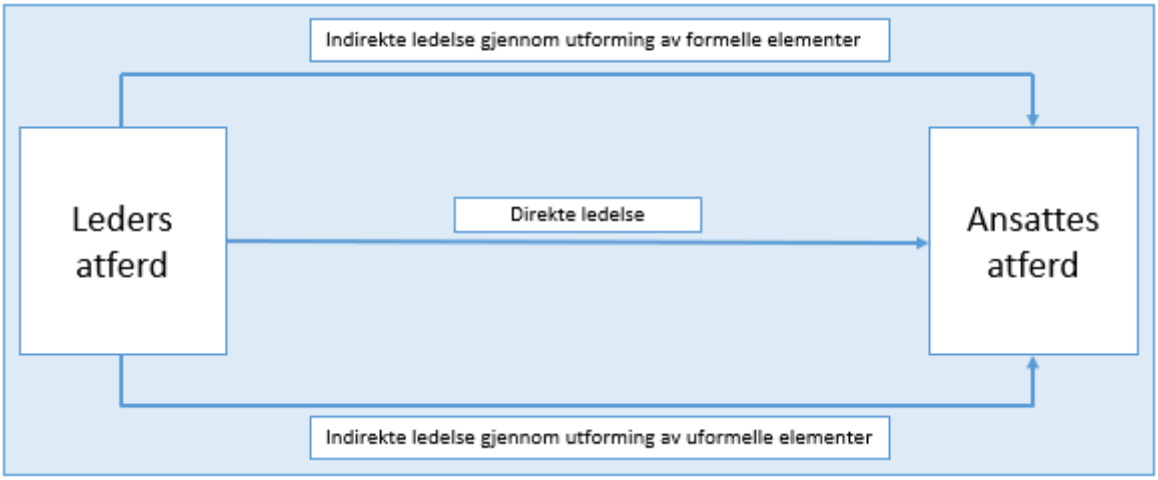
Elektroniske kanaler er relevant for dagens virksomheter da mye av dagens kommunikasjon foregår på denne måten. På hjemmekontor prater man med kollegaer og ledere ved bruk av videomøter, chat og e-post. Dette kan ha betydning for informasjonen som deles mellom kollegaene. Det har også betydning for hvordan en tolker den informasjonen man er gitt. I tillegg gjør elektroniske kanaler det vanskelig å oppfatte kroppsspråk, og hindrer flyt i samtalen (Kaufmann & Kaufmann, 2014, s. 292). Det kan derfor være utfordrende å drive god ledelse, og å skape organisasjonskultur gjennom elektroniske kanaler.

2.5 Ledelse

Ledelse har eksistert like lenge som mennesket selv, og fram til 1800-tallet var en leders rolle å kontrollere de underordnedes atferd. Da industrialiseringen skjøt fart rundt 1880 ble det lagt større vekt på å vedlikeholde underordnedes sosiale system (Haukdal-Brochs, 2011, s. 21). Fra 1970 har ledelse derimot dreid seg om å støtte medarbeidernes utvikling, og å forstå ledelse som relasjoner mellom en leder og dens ansatte (Sagberg, 2021). I dag kan en beskrive ledelse som en spesiell atferd for å påvirke andre menneskers tenking, holdninger og atferd. Å lede ansatte i en virksomhet dreier seg som regel om å motiver disse til å yte sitt beste for å realisere virksomhetens mål. Ledelse utføres av en eller flere personer, formelt kalt «*ledere*», men det kan også utføres uten gitte titler, med hensikt i å påvirke andre til å gjøre noe for seg selv eller virksomheten. Det er altså viktig å kunne skape ønsket atferd hos sine ansatte gjennom godt lederskap, og ved å benytte ulike teknikker for å oppnå dette (Kaufmann & Kaufmann, 2014, s. 334). Teori om ledelse er svært relevant for alle virksomheter, da dette har stor innvirkning på de ansattes atferd.

2.5.1 Direkte og indirekte ledelse

En kan påvirke organisasjonsatferd direkte og indirekte som vist i figur 2.6. All samhandling og kommunikasjon mellom ledere og dens ansatte vil være en form for direkte ledelse. Indirekte ledelse vil derimot være alle måter en leder kan påvirke organisasjonsatferden uten direkte samhandling. Denne teorien kan deles inn i to hovedtyper. Først og fremst kan en påvirke sine ansatte ved bruk av mål, strategi og organisasjonsstruktur, samt ved formelle program for rekruttering, opplæring og sosialisering. Denne formen for indirekte ledelse utformes via formelle elementer. Indirekte ledelse brukes også gjennom utvikling av organisasjonskultur. Dette ved å styrke de ansattes verdier og normer, eller ved å endre disse. Å påvirke ansattes verdier og normer gjennom utvikling av kultur er indirekte ledelse med uformelle elementer (Jacobsen & Thorsvik, 2016, s. 417).



Figur 2.6 – Direkte og indirekte ledelse (Jacobsen & Thorsvik, 2016, s. 417)

Denne teorien er relevant siden dirkete og indirekte ledelse sier noe om ledernes påvirkningskraft. Indirekte ledelse kan bli spesielt utfordrende i virksomheter der de ansatte nå benytter hjemmekontor. Dette kan på lang sikt utfordre den allerede eksisterende kulturen i virksomheten.

2.5.2 Ledelse i virtuelle organisasjoner

Informasjons- og kommunikasjonsteknologi har gjort det mulig å effektivt lede en virksomhet der ansatte og ledere er geografisk atskilte. Dette viste seg å bli spesielt aktuelt i mars 2020, da store deler av Norges befolkning ble plassert på kontor i sine egne hjem. Virtuelle team er personer som arbeider sammen, men som ikke er i fysisk kontakt (Kaufmann & Kaufmann, 2014, s. 236). Dette er fordelaktig fordi en kan sette sammen

eksperter uavhengig av sted og tidssoner. Allikevel kan denne form for samarbeid resultere i anonyme ansatte, som yter og bidrar mindre enn om de hadde vært til stede fysisk i organisasjonen. Økt konfliktnivå mellom ansatte, samt mangel på de rette kanalene å håndtere dette på, gjør også virtuelle team til en utfordring. Effektiviteten i teamet er best når en fra før av kjenner de man jobber sammen med. Altså vil ansatte som aldri har møtt hverandre før være mindre effektive (Einarsen & Martinsen, 2019, s. 247;248).

Den største utfordringen for ledere i virtuelle organisasjoner er fysisk avstand, og mangel på ansikt- til- ansikt-kommunikasjon. Når en er fysisk atskilt og kommuniserer elektronisk, kan det føre til sosial fragmentering. En vil dermed ha utfordringer med å utvikle en organisasjonskultur der de ansatte føler samhold og tilhørighet. På bakgrunn av problemene som kan oppstå med virtuelle team må en som leder legge stor vekt på relasjonsbygging, samt det å kjenne til muligheten ulik type teknologi vil gi de ansatte og virksomheten (Einarsen & Martinsen, 2019, s. 248).

Denne teorien er spesielt relevant for virksomheter da det i år 2020 ble nødvendig med hjemmekontor på bakgrunn av koronapandemien. Hjemmekontor kan gi ledelsen utfordringer knyttet til å skape en god sikkerhetskultur. For eksempel kan nye ansatte med lite sikkerhetsopplæring føre til dårlig vaner og holdninger. Derfor vil god ledelse være spesielt viktig i situasjoner der ansatte er geografisk atskilt.

2.5.3 John Kotters endringsmodell

John Kotter har registrert åtte fokusområder en leder bør ha når en skal gjennomføre en endring. Han observerte flere organisasjoner over en lang tidsperiode, og identifiserte deres suksessfaktorer som nå har blitt til endringsmodellen (Kotter International, 2021). Trinnene i modellen er viktige på hver sin måte for å kunne gjennomføre en endringsprosess med minst mulig motstand, og Kotter mener en skal følge disse stegene systematisk for å oppnå en vellykket endring (Einarsen & Martinsen, 2019, s. 440). Dette har vi presentert i figur 2.7.

Figur 2.7 – John Kotters endringsmodell (Kotter International, 2021), vår oversettelse

Å skape et *endringsbehov* er det første trinnet i modellen. En må bevise for de ansatte i organisasjonen at endring er nødvendig. Dersom en ikke ser behovet vil det lett oppstå motstand, og derfor er det vesentlig at en kommuniserer på en motiverende og engasjert måte (Jacobsen, 2018, s. 220). Videre skal en bygge et *veiledende team*, gjerne av allerede motiverte ansatte. Disse vil være med å fremme endringen ut i organisasjonen. For å skape engasjement for endring sier Kotter at en må ha en strategisk og tydelig *visjon*, som alle i organisasjonen forstår. Videre må visjonen *kommuniseres* ut i virksomheten, gjerne via ulike kommunikasjonskanaler. Endringsteamet kan være et godt virkemiddel for å spre budskap og engasjement raskt. Det femte punktet i John Kotters modell handler om å *fjerne hindringer* og motstand. Endringsprosesser vil nesten alltid møte motstand, men det er viktig å minimere dette i så stor grad som mulig (Bolman & Deal, 2018, s. 449). *Tidlig suksess* og anerkjennelse fungerer som en motivasjonsfaktor for alle i en organisasjon. Å sette kortsiktige mål på vei mot visjonen er derfor et godt virkemiddel for

å opprettholde fokuset. En endringsprosess kan være tidkrevende, og etter hvert blir det vesentlig for ledelsen å holde de ansattes *tempo og fokus oppe*. Det tar tid å endre arbeidsflyt, kultur og vaner, noe som en endringsprosess gjerne medfører. Modellens siste punkt forteller at en skal *forankre endringen*. For at en endring skal være vellykket, kan ingen i organisasjonen gå tilbake til gamle vaner og rutiner (Kotter International, 2021). Dette er en tidkrevende prosess, men en kan ikke definere en endring som forankret før alle de ansatte har kommet godt inn i nye rutiner.

Når en organisasjon går gjennom en endringsprosess, vil en ved å ta utgangspunkt i Kotters åtte steg for vellykket endring kunne oppleve en enklere prosess. Teorien er derfor svært relevant for organisasjoner i endring.

3 Metode

Det skilles mellom to ulike begreper når det kommer til datainnsamling og analyse, *primærdata* og *sekundærdata*. Primærdata er data en samler inn på egenhånd for å besvare et gitt problem. Ved primærdata innhenter man informasjon ved hjelp av observasjon eller intervju. Sekundærdata er derimot allerede eksisterende datakilder som en benytter for å støtte opp om egne funn (Sundbye & Nisted, 2017). Datainnsamlingsmetoden deles inn i kvalitativ og kvantitativ metode. Kvalitativ metode innebærer å benytte seg av data en har innsamlet til analyse. Resultatene fra slike metoder blir utformet i tekst (Grønmo, 2020a). Ved kvantitativ metode benytter en seg også av innsamlet data, men her blir resultatet presentert som tall og statistikk (Grønmo, 2020b).

I forbindelse med vår oppgave valgte vi å ta utgangspunkt i Tor Busch (2019) sin tilnærming til akademisk skriving, og de forskningsmetodene som fremkommer i denne boken. Henholdsvis valg av vitenskapsteoretisk utgangspunkt, valg av forskningsdesign, valg av metoder for datainnsamling og valg av metoder for dataanalyse. Disse er knyttet sammen og vil derfor påvirke hverandre i stor grad. Med utgangspunkt i disse temaene har vi klare retningslinjer for hvordan vi ønsker å samle inn data som besvarer vår problemstilling.

3.1 Vitenskapsteoretisk utgangspunkt

Det vitenskapsteoretiske utgangspunktet er et overordnet spørsmål en tar stilling til, når en skal utføre vitenskapelige undersøkelser. Dette utgangspunktet legger føringer for senere metodevalg og analyse. For denne oppgaven har vi valgt hermeneutikk, som er et fortolkningsbasert utgangspunkt. Dette utgangspunktet sier *«at fokuset settes på å tolke meningsinnholdet i de tekstene eller ytringene som avdekkes gjennom en vitenskapelig undersøkelse»* (Busch, 2019, s. 51). En forstår andre mennesker ved å tolke det som blir formidlet, hvor en fokuserer på å skape en helhet rundt forskningsspørsmålet (Patel & Davidson, 1999, s. 26). I denne oppgaven er vi avhengig av å kunne tolke resultatene fra intervjuene, og knytte disse mot relevant teori for å besvare problemstillingen.

Når det kommer til forskning, skilles det gjerne mellom to tilnærminger. Disse tilnærmingene er induktiv og deduktiv tilnærming. Induktiv tilnærming forekommer når en ikke har en bestemt hypotese om empiri og teori på forhånd. Deduktiv tilnærming tar utgangspunkt i eksisterende empiri og teori, og gjennom forskningen vil en kunne avgjøre hvorvidt hypotesen stemmer eller ikke (Bø, 1995, s. 25;26). Før prosjektet startet, var det en underliggende hypotese om at virksomhetens sikkerhetsinstruks ikke var i samsvar med virksomhetens verdier. Vi hadde derimot ingen data å ta utgangspunkt i. Vår forskning er derfor en blanding av induktiv og deduktiv, og betegnes av Busch (2019, s. 51) som en abduktiv tilnærming. I denne tilnærmingen beveger en seg dynamisk mellom empiri og teori, og utgangspunktet blir derfor endret underveis.

3.2 Forskningsdesign

Valg av hoveddesign baserer seg på det vitenskapsteoretiske utgangspunktet, samt valg mellom ekstensivt eller intensivt design, kvalitative eller kvantitative metoder, og oppgavens tidsperspektiv. Ved et ekstensivt design blir data samlet inn fra mange kilder, mens en i et intensivt design samler en data fra et fåtall kilder (Busch, 2019, s. 52). Vi valgte å gå for et intensivt design, og gjennomførte derfor intervjuer med noen utvalgte ansatte hos HelseIT. Dette ga oss relevant data for å besvare oppgavens problemstilling. Ved å diskutere temaet med noen få utvalgte, ga dette oss et godt innblikk i hvordan sikkerhetsinstruksen blir behandlet i praksis, samt hvordan virksomhetens sikkerhetskultur er. Dette ga oss et godt datagrunnlag, spesielt da informantene hadde ulik utdanningsbakgrunn og ansvarsområder. I utgangspunktet hadde vi planlagt å gjennomføre en spørreundersøkelse for å i større grad kartlegge organisasjonens helhetlige holdninger. Vi mener vårt datagrunnlag fra intervjuene derimot er godt nok til å besvare vår problemstilling, og vi gikk derfor bort ifra spørreundersøkelse. Dette da utarbeidelsen er svært krevende, og en ikke har mulighet til å gjøre endringer etter undersøkelsen er sendt ut. Spørsmålene kan tolkes ulikt for hver respondent, og det vil derfor kunne være mer usikkerhet knyttet til resultatet. I et intervju vil en derimot kunne oppklare eventuelle usikkerheter rundt spørsmålene, samt ha muligheten til å besvare disse mer utfyllende.

Da oppgaven vår kun skrives på ett semester, var vi nødt til å gjennomføre en tverrsnittsundersøkelse. Dette betyr at en samler inn data på ett tidspunkt. Denne

metoden er en effektiv måte å samle, bearbeide og analysere informasjon på når en har lite tid. Det hadde likevel vært interessant å samle inn data på ulike tidspunkt, og gjerne med noen måneders mellomrom. Dette for å se om vår problemstilling bidro til å skape mer kunnskap og innsikt om sikkerheten i bedriften etter intervjuene var gjennomført.

3.2.1 Hoveddesign

Ved valg av hoveddesign for denne oppgaven, vil både vitenskapelig utgangspunkt og forskningsdesign være viktige faktorer. Da vi skulle velge oppgavens hoveddesign sto det mellom casestudie og aksjonsforskning. Aksjonsforskning er en metode der forskerne deltar som aktør i en endringsprosess, og det kjennetegnes ved at en veksler mellom datainnsamling, analyse, felles refleksjon og handling (Busch, 2019, s. 56). Da vi har begrenset tid og innflytelsesrett hos virksomheten blir aksjonsforskning lite aktuell. På bakgrunn av dette har vi valgt casestudie. Casestudien bygger på målrettede undersøkelser, basert på et teoretisk utgangspunkt. Fenomenet som studeres knyttes opp mot den spesifikke virksomheten, og en er derfor avhengig av riktig kontekst (Busch, 2019, s. 56). I vårt tilfelle vil sikkerhetsinstruks, samt kultur, variere fra virksomhet til virksomhet. Det er derfor lite gunstig å ta utgangspunkt i en annen bedrift, og en må gjøre undersøkelser i den aktuelle virksomheten for at fenomenet skal kunne forstås. Askheim og Grennes (2018, s. 70) sier at en kan velge case når «*det er typisk for det feltet vi jobber innenfor*». Dette vil da være med på å legitimere resultatenes overførbarhet til andre virksomheter. Resultatene vil være spesifikke fra casebedriften, men kan benyttes som et verktøy for å øke den generelle kunnskapen rundt problemstillingen.

3.3 Utvikling av problemstilling

Vår problemstilling har fremkommet som et resultat av en iterativ prosess. Da vårt vitenskapelige utgangspunkt har en abduktiv tilnærming, lot dette seg gjøre. Dagens problemstilling oppsto gjennom dialog med HelseIT, samt aktiv bevegelse mellom empiri og teori. Høsten 2020 kom vi i samarbeid med HelseIT frem til at vi ville forske på virksomhetens personlige datasikkerhet. I utgangspunktet ønsket vi å besvare *«hva kan ledelsen gjøre for å bedre de ansattes personlige sikkerhet?»*, men etter det første møtet i 2021 fant vi ut at de ansatte i utgangspunktet har hatt et godt forhold til området. Etter å ha lest igjennom virksomhetens sikkerhetsinstruks, og funnet et stort forbedringspotensial, ville vi trekke denne inn i oppgaven. Det har hele veien vært viktig

at vårt arbeid skulle være av nytte for HelseIT, og derfor utviklet problemstillingen seg videre til *«hvordan kan sikkerhetsinstruksen brukes som et kommunikasjonsverktøy?»*. Dette var vårt utgangspunkt da intervjuguiden ble utarbeidet, og vårt hovedmål for de første intervjuene.

Under intervjuene registrerte vi derimot et dårligere fokus på personlig datasikkerhet på hjemmekontor. Etter et møte med HelseIT ble dette området trukket frem som interessant, og arbeidet med en ny problemstilling startet. Vi ønsket å kartlegge forskjellen mellom nyansatte under koronapandemien, samt ansatte med et lengere arbeidsforhold. Siden koronapandemien har medført hjemmekontor, ble det viktig for oss å inkludere dette i problemstillingen. Dette da pandemien er med på å påvirke de ansattes atferd, da den tvang frem en hjemmekontorløsning. Vi la dermed til noen spørsmål i intervjuguiden som i større grad fokuserte på atferd på hjemmekontor. Samtidig ville vi fortsette å se på virksomhetens sikkerhetsinstruks, og spesielt da det ble tydelig at deres opplæringsrutiner rundt sikkerhet er blitt påvirket av koronapandemien. I samsvar med både veileder og HelseIT, kom vi frem til oppgavens problemstilling: *«Hvordan kan en sikkerhetsinstruks påvirke en organisasjon i endring under koronapandemien?»*.

3.4 Innsamling av data

I dette delkapittelet presenterer vi metoden som ble benyttet for å samle inn data. Vi har benyttet kvalitativ metode, i form av intervju, for å innhente data. Teorigrunnlaget i kapittel 2 er også en kvalitativ metode vi har benyttet oss av.

3.4.1 Intervju

Intervju er den kvalitative metoden vi benyttet oss av for å innhente data. Vi valgte en semistrukturert form, hvor hovedmålet var å ha en samtale med informantene rundt et tema (Andersen, 2020). Formålet var å få innsikt og dybdekunnskap om meninger, holdninger og normer rundt personlig sikkerhet og kultur. Intervjuguiden (Vedlegg 1) ble i stor grad benyttet som en temaguide basert på problemstillingen, hvor vi skrev ned noen spørsmål rundt temaet vi ville diskutere. På denne måten hadde vi noen spesifikke spørsmål vi kunne stille, dersom samtalen stoppet opp. Intervjuguiden er felles for alle informantene, men den ble tilpasset noe avhengig av stillingsforhold. Fordelen med

semistrukturert intervju er at en kan få informasjon en ikke nødvendigvis har tenkt på tidligere. Ved å stille åpne spørsmål, vil det være rom for refleksjon og diskusjon. Intervjuene vil i stor grad være forskjellige for hver informant, fordi en får ulike innfallsvinkler. Ved et semistrukturert intervju har en mulighet til å stille oppfølgingsspørsmål, slik at informanten kan utdype de meningene informanten kommer med.

I samarbeid med HelseIT ble vi enige om passende informanter. Vi ønsket å komme i kontakt med ansatte med ulik utdanningsbakgrunn, alder og stillingsforhold. Med dette som utgangspunkt ble vi satt i kontakt med både nyansatte, og ansatte som har jobbet hos virksomheten siden oppstart. Vi valgte å gjennomføre individuelle intervjuer. Dette fordi vi ønsket personlige erfaringer, tanker og meninger, og lite påvirkning fra andre ansatte. Ved innkallelse ble ikke intervjuguiden lagt ved, noe som var et bevisst valg vi tok, da vi ikke ønsket at informantene skulle gå igjennom sikkerhetsinstruksen på forhånd. Det ble derfor kun presentert tema for intervjuet i innkallelsen, slik at vi kunne få et inntrykk over hvordan sikkerhetsinstruksen ble tatt hensyn til i hverdagen.

Informant 1	Har jobbet for HelseIT i 10 år som HR-rådgiver. Arbeidsoppgaver som omhandler systemer, prosesser og rutiner. Språk- og samfunnsfaglig utdanning.
Informant 2 *Nøkkelinformant*	Har jobbet for HelseIT i 2 og et halvt år som sikkerhetsdirektør. Ansvar for HelseCERT *(helsesektorens felles kompetansesenter for IKT-sikkerhet)*, og er sikkerhetsleder for selskapets helhet *(operativt sikkerhetsarbeid)*. Ingeniør med master i kommunikasjonsteknologi og informasjonssikkerhet. Doktorgradsstipendiat hos NTNU.
Informant 3	Har jobbet for HelseIT i et halvt år som sikkerhetsleder. Ansvar for helseforvaltning, samt et internt fagansvar. Bachelorgrad i Drift av datasystemer. Pågående mastergrad i Organisasjon og ledelse.
Informant 4	Har jobbet for HelseIT i et og et halvt år som lønnskonsulent. Arbeidsoppgaver med basis i lønn. Deltidsstudium i lønnsmedarbeider.
Informant 5	Har jobbet for HelseIT i fem år, og startet som lærling. Jobbet tidligere som brukersupport, men nå med internt system og brukerstøtte. Arbeidsoppgaver som omhandler brukerstøtte til ansatte, samt scripting og drifting av servere. Yrkesfaglig utdanning på IKT-linje med fagbrev.
Informant 6	Har jobbet for HelseIT i et halvt år som rekrutteringskoordinator. Arbeidsoppgaver som omhandler rekruttering av nye ansatte. Bachelorgrad i markedsføring, og årsstudium i samfunnsøkonomi.

Tabell 3.1 – Oppgavens informanter

Grunnet koronapandemien ble intervjuene gjennomført via Microsoft Teams. Vi startet intervjuene ved å presentere oss, samt å forklare formålet med intervjuet og at vi ønsket et så åpent og ærlig svar som de kunne gi. Før intervjuet ble det sendt ut en samtykkeerklæring (Vedlegg 2), som ble bekreftet via e-post. Før intervjuet forsikret vi oss allikevel om at samtykket var godkjent, og at det ikke var noen spørsmål i tilknytning til samtykkeerklæringen. De første spørsmålene var generelle, hvor informanten fikk presentere seg selv, dens tanker rundt personlig sikkerhet, hvilke opplæring som var blitt gitt, og hvordan holdningene til personlig sikkerhet var i virksomheten. Videre ble spørsmålene rettet mer spesifikt rundt sikkerhetsinstruksen. Dette omhandlet blant annet om hvordan de oppfattet hensikten, hva de tenkte rundt instruksen, og hvorvidt den var motiverende eller ikke. Vi avsluttet intervjuene ved å spørre om informanten hadde noen innspill, eller noe de ville dele utover det som kom frem av intervjuet.

Intervjuene hadde en varighet på 20-40 minutter, og vi takket hver informant for gode innspill og deltakelse ved intervjuets slutt.

I etterkant av intervjuene startet prosessen med å transkribere, som betyr å overføre tale til skrift (Gundersen, Johansen, & Bjerkestrand, 2018). Hensikten med en slik prosess er å få en direkte avskrift av det informantene har sagt, som gjør det enklere å analysere dataen i ettertid. Det ble tatt opptak av intervjuene via Microsoft Teams, slik at vårt fokus kunne være på informantene mens intervjuet foregikk. Vi ble enige om hvordan vi skulle gjøre transkriberingen på forhånd, og fordelte dermed intervjuene mellom hverandre. På denne måten ble transkriberingen relativt lik, og prosessen gikk fortere.

Da alle intervjuene var transkribert startet prosessen med å analysere dataene. Dette var en kontinuerlig iterativ prosess hvor vi gikk igjennom hvert intervju flere ganger. Grunnet oppgavens fortolkningsbaserte utgangspunkt fokuserte vi på å tolke informantenes besvarelse. Dataen fra alle informantene ble sortert og kategorisert i et Excel-ark. Dette var for å enkelt få oversikt over eventuelle likheter og ulikheter, samt å skape et grunnlag for resultatkapittelets inndeling. Etter en overordnet sortering begynte arbeidet med å finne sitater og data som var i direkte tilknytning til oppgavens problemstilling. Disse dataene samlet vi videre i et nytt Excel-ark, og gjorde arbeidet med resultatdelen mer oversiktlig.

3.4.1.1 Behandling av intervjudata

Samhandlingsplattformen Microsoft Teams ble benyttet i forbindelse med intervjuene. Denne plattformen ble valgt for å ivareta informantenes personvern. Opptakene ble lagret i tilgangskontrollerte systemer som NTNU har databehandleravtale med, jf. Personvernforordningen (Personopplysningsloven, 2018, §1). Opptakene og transkripsjonen håndteres etter innmelding til Norsk senter for forskningsdata. Etter prosjektslutt, vil data i forbindelse med intervjuene bli slettet.

3.5 Metodekvalitet

Våre valg knyttet til metode påvirker oppgavens kvalitet. God metodekvalitet er viktig for å sikre resultatets troverdighet, og det er særlig tre momenter som påvirker dette: pålitelighet, gyldighet og overførbarhet. Pålitelighet dreier seg om korrekt informasjon,

og et resultat en kan være trygg på. Gyldighet omhandler i hvilken grad dataen vi innhenter, analyserer og måler faktisk er det vi ønsker å måle basert på problemstillingen. Med overførbarhet menes det om resultat kan overføres til andre situasjoner (Busch, 2019, s. 62). Malterud (2003), referert i Berntsen (2019), presenterer fire hovedkrav til vitenskapelighet. Disse kravene inkluderer de tre momentene til Busch (2019), men går noe mer i dybden da det kommer til metodekvalitet og kritisk tenkning. De fire hovedkravene er egnet for både kvantitative og kvalitative metoder. Hovedkravene presenteres i listen under, og i diskusjonsdelen vil vi se tilbake på kravene for å forsikre at resultat og konklusjon tilfredsstiller disse. Delkapittel 3.5.1 som omhandler kildekritikk vil også være med på å reflektere rundt oppgavens troverdighet.

1. *Systematisk kritisk refleksjon*

Det første kravet handler om hvorvidt resultatet kan overføres til andre situasjoner eller ikke. Dette innebærer i hvilken grad kunnskapen oppgaven presenterer er gjenbrukbar.

2. *Relevans*

Dette kravet sier noe om hva kunnskapen kan brukes til. Her ser en på hvorfor akkurat dette arbeidet er relevant. En legger stor vekt på originalitet da kunnskapen skal bidra til noe nytt, eller unikt.

3. *Validitet – gyldighet og pålitelighet*

Det er viktig å undersøke hva en faktisk har kommet fram til, og en ser derfor på kravet om validitet. En ser her på om resultatet er logisk korrekte, og om det er riktig i forhold til konteksten. Dette kravet sier også noe om resultatet er konsistens, og at resonnementet har en klar sammenheng.

4. *Refleksivitet*

Det siste kravet som presenteres er krav om refleksivitet. Dette omhandler hvordan forskningsprosessen har preget oppgavens analyse og konklusjon. Faktorer som kan påvirke dette er subjektivitet, objektivitet, skjevhet og fordomsfullhet. For kvalitative forskningsmetoder har disse faktorene særlig betydning for oppgavens troverdighet.

Malterud (2003), referert i Berntsen (2019)

3.5.1 Kildekritikk

Vi gjennomførte intervju med seks informanter, hvor temaet var personlig datasikkerhet. Det vil alltid være en risiko at informantene svarer ugyldig, eller fremmer seg selv mer positivt enn realiteten. Spørsmål rundt personlig sikkerhet kan oppfattes som sensitivt, og derfor har vi forsøkt å skape et gyldig resultat ved å stille oppfølgingsspørsmål. Ved at vi valgte semistrukturert intervjuform lot dette seg gjøre. Da vi intervjuet seks informanter, fra ulike avdelinger, fikk vi et mer tydelig bilde på hvordan virksomheten er som helhet. Resultatet vårt vil derimot være påvirket av at vi ikke hadde mulighet til å kartlegge en større del av virksomheten. Samtidig fikk vi ikke mulighet til å intervjue mer enn to nyansatte, noe som kan være en svakhet for oppgaven. Vår oppgave vil med dette være begrenset til disse informantenes svar.

For vårt teorikapittel har vi benyttet oss av eksterne kilder. Vi har i stor grad brukt fagbøkene «*Hvordan organisasjoner fungerer*» av Dag Ingvar Jacobsen og Jan Thorsvik, «*Organisasjon og ledelse*» av Ståle Valvatne Einarsen og Øyvind Lund Martinsen, samt «*Psykologi i organisasjon og ledelse*» av Geir og Astrid Kaufmann. Samtidig har vi benyttet oss av andre relevante fagbøker for å skape en større dybde i oppgaven. Fagbøkene vi har benyttet er relativt nye, da vi ønsket et så nytt perspektiv på teorien som mulig. For vårt metodekapittel har vi i hovedsak benyttet fagboken «Akademisk skriving for bachelor og masterstudenter» av Tor Busch, med supplering fra andre fagbøker og artikler. Ved innhenting av informasjon og data fra ulike webområdet kan informasjon være publisert og redigert av hvem som helst. Dette er grunnen for at vi i hovedsak har benyttet oss av fagbøker. Vi har allikevel benyttet oss av digitale kilder, og vi har da kontrollert kildens gyldighet. I hovedsak er disse kildene hentet fra Norsk digital læringsarena, Store norske leksikon, samt større organisasjoner med god kunnskap rundt de ulike områdene.

4 Resultater

I dette kapittelet vil vi presentere resultatene fra oppgavens datainnsamling. Innsamlingen er gjort fra seks semistrukturerte intervjuer av informanter fra forskjellige avdelinger i virksomheten. Etter en analyse av hvert intervju, har vi valgt å presentere resultatene i fem delkapitler vi mener er svært relevant for oppgavens problemstilling. Det er kun de mest interessante og relevante dataene som fremkommer i dette kapittelet.

4.1 Dagens sikkerhetsinstruks

Ved spørsmål om hva en sikkerhetsinstruks innebærer svarer de fleste informantene at det er et dokument som sier noe om hvordan en som ansatt skal forholde seg til sikkerhet. Andre sier det er noe en signerte da man startet i virksomheten. Dette tyder på at de forstår hva dokumentet innebærer. Informantene forteller at dokumentet fungerer som en formalitet, og legger et ansvar på hver enkelt ansatt i HelseIT. Med ansvar menes ansvarliggjøring av eventuelle brudd på sikkerhetsinstruksens innhold. Våre funn viser at innholdet i sikkerhetsinstruksen ikke gjenspeiler det som er viktig for organisasjonen, og at den er lite målrettet. HelseIT har hatt et stort fokus på å utvikle et ISMS, mens arbeidet med sikkerhetsinstruksen har falt noe bort. Ved utarbeidelse av ISMS er det lagt stor vekt på beskrivelse av hvilket formål sikkerhetsarbeidet har. Det blir fremmet hvilken rolle organisasjonen har i samfunnet, deres samfunnsoppdrag og betydningen av et godt sikkerhetsarbeid. Dette er noe sikkerhetsinstruksen ikke fremmer, og den er derfor ikke like formidlende som annen dokumentasjon. En ideell sikkerhetsinstruks for HelseIT bør stå i samsvar med hvordan styringssystemet for informasjonssikkerhet er lagt frem.

Én informant kunne ikke huske å ha lest, eller signert, instruksen. Flertallet forteller derimot at de både har signert og forstått den, men det er allikevel ingen som kan si hva instruksen inneholder. Dette viser at instruksen har et stort forbedringspotensial. Samtidig blir den fremstilt som generisk. Dette kan tyde på at en ikke føler en slags relevans til innholdet i instruksen, sammenlignet med reell arbeidshverdag, da den leses igjennom. Dette kan bety at det ikke er alle ansatte som har forstått innholdet.

«Hvis vi virkelig ønsker at den ansatte skal forstå det, og forstå hva som er viktigst i hverdagen, så er den ikke et godt verktøy.» ***Informant 2***

Det kommer frem av våre funn at det i større grad er andre verktøy som har gjort informantene bevisst over egen sikkerhet. Dette gjelder spesielt for de med et lengre arbeidsforhold. Forskjellige kurs, nyansattsamlinger og erfaring blir sett på som en bedre metode for å bevisstgjøre rundt datasikkerhet. Disse resultatene kan tyde på at sikkerhetsinstruksen i dag er lite motiverende, med et innhold det er vanskelig å sette ut i praksis.

"Jeg er veldig sikker på at jeg forsto innholdet der og da, men om jeg husker det er en annen sak [...] Så for min del har det ikke vært sånn at jeg har lest og forstått [...] men heller bygget litt opp gjennom årene."
Informant 5

Sikkerhetsinstruksen fremmer ikke et budskap som gjenspeiler virksomhetens verdier slik som den er i dag, og den har ikke blitt revidert på mange år. Dokumentet inneholder blant annet ingen informasjon om sårbarheter via e-post, eller på hjemmekontor. Den nevner dog elementer som hvordan håndtere passord og datamaskin, samt hvordan en skal forholde seg til internett.

På spørsmål om hvordan sikkerhetsinstruksen kan forbedres nevner alle informantene «*tilgjengelighet*». Det er kun én informant som etter litt tid klarer å finne instruksen på intranettet. Samtidig nevner de fleste at en burde lese igjennom, samt godkjenne, sikkerhetsinstruksen med jevne mellomrom. Rundt halvparten av informantene mener instruksen i større grad må fremme de verdiene virksomheten står for. Dens budskap må samtidig gjentas, slik at en kan skape gode holdninger for datasikkerhet. Våre funn viser også etterspørsel av andre metoder for å fremme viktigheten av personlig sikkerhet. Det fremkommer at sikkerhetsinstruksen er krevende å lese igjennom. Dette tyder igjen på at instruksens struktur og formulering, slik som den står i dag, hverken er god, interessant eller motiverende.

4.2 Sikkerhet på organisatorisk, teknisk og personlig nivå

Ut ifra resultatene kategoriserte vi de ansattes vaner og holdninger om personlig sikkerhet inn i tre nivåer: organisatorisk, teknisk og personlig nivå. Med organisatorisk menes de sikkerhetstiltakene som gjennomføres fra organisasjonen. Det tekniske nivået tilsvarer teknologi, mens det personlige nivået beskriver de tiltakene hver enkelt ansatt gjennomfører når det kommer til seg selv og egne arbeidsprosesser. Av intervjuene er det registrert ulikheter mellom hvilke tiltak som gjennomføres fysisk på kontoret, og de som gjøres under koronapandemien på hjemmekontor. Derfor presenterer vi tiltakene på hjemmekontor i et eget avsnitt.

4.2.1 Organisatorisk

På organisatorisk nivå har virksomheten taushetserklæringer, tilgangsstyring og et regelverk rundt personvern. De organisatoriske sikkerhetstiltakene blir nevnt av informantene som jobber i HR og lønn. Her nevnes også åpne kontorlandskap, og at de har lukkede rom en kan benytte dersom konfidensielle samtaler skal gjennomføres. Særlig trekkes HelseCERT frem under organisatorisk sikkerhet. HelseCERT svarer på eventuelle spørsmål som oppstår vedrørende sikkerhet. Vi har ingen funn rundt spesielle tiltak til sikkerheten på hjemmekontor på organisatorisk nivå. Allikevel er taushetserklæring og tilgangsstyring fremdeles relevant når de ansatte sitter hjemme.

4.2.2 Teknisk

På teknisk nivå fremkommer det at HelseIT har dører med kodelås, som stenges etter klokken 16:00. Dette er et tiltak for å hindre uautorisert tilgang. En jobber også i egne systemer som krever tofaktorautentisering, med gode løsninger for tilgangsstyring. Det er derimot kun informantene med IKT-bakgrunn som sier de har gode løsninger for håndtering av passord og annen sensitiv informasjon.

Av tekniske tiltak utover de som er nevnt har kun en av informantene gjort tilpasninger av sitt eget nettverk hjemme for å være sikker på at ingen uvedkommende bryter seg inn. Informanten har stor interesse for informasjonssikkerhet, og dette er en av hovedårsakene til tiltaket. Basert på våre funn har altså kun én informant gjennomført ytterligere tekniske tiltak på hjemmekontor. HelseIT har derimot tekniske

sikringsmekanismer innebygd i alt utstyr. Dette er et tiltak som er blitt gjort, slik at sikkerheten skal være god uavhengig av hvilket nettverk en sitter på. Dette innebærer sikringstiltak på klient, slik som VPN mot HelseIT sitt nettverk, kryptering av harddisker og lokale brannmurer. På denne måten er ikke de ansatte avhengig av å eksempelvis ha et godt sikret nettverk hjemme for å jobbe sikkert.

4.2.3 Personlig

Våre funn viser at de ansatte er klar over viktigheten av å låse skjerm for å motvirke innsyn fra uvedkommende. På et personlig nivå er det samtidig noen informanter som nevner e-post, og at en er bevisst over at alt ikke nødvendigvis er slik det fremstår. Av informantene ble dette særlig nevnt av de med et lengre ansettelsesforhold, hvor informasjonen om personlig datasikkerhet er blitt gitt ved andre metoder enn sikkerhetsinstruksen. På HR-avdelingen registrer vi et spesielt godt fokus på taushetserklæringer. Det snakkes ofte i koder mellom hverandre, da en også har interne taushetserklæringer innad i organisasjonen. Våre resultater viser at taushetserklæring er det området informantene på HR og Lønn spesielt legger vekt på, da en snakker om datasikkerhet. Dette kan dog tyde på at en ikke er helt sikker på hva begrepet innebærer. Kun to av informantene har et bevisst forhold til bruk av sosiale medier, og hvordan det kan påvirke virksomheten.

> *«[…] jeg har jo satt opp HelseIT som arbeidsplass på Facebook. Så hva jeg på en måte ytrer og gjør der gjenspeiler jo litt på organisasjonen, og kan gå utover de.»* ***Informant 6***

På hjemmekontor er det svært få tiltak som gjennomføres, og de fleste informantene forteller at de ikke tenker like mye på personlig sikkerhet da de er hjemme. Tiltak som eksempelvis skjermsparer blir lite brukt, men noen nevner at de er flinkere dersom de ikke er alene. Våre resultater viser at en i større grad føler seg tryggere i eget hjem. Samtidig kan det virke som at en glemmer datasikkerhet, nettopp fordi en sitter hjemme. Å lukke vinduet dersom en skal i et møte, eller gjennomføre en telefonsamtale, blir nevnt av et par informanter som et tiltak en gjør på hjemmekontor. Basert på våre funn mener

vi derimot at det generelt sett er lav datasikkerhet på et personlig nivå når en arbeider hjemmefra.

«Det er egentlig mindre siden jeg er i mitt eget hus [...] Er egentlig bare mer frihet, og litt mindre sikkerhet.» ***Informant 5***

4.3 Sikkerhetsopplæring

Vi valgte å kategorisere virksomhetens sikkerhetsopplæring i formell og uformell opplæring. Ved formell opplæring mener vi de opplæringsrutinene som er arrangert for ansatte i forbindelse med deres arbeidsoppgaver i virksomheten. Uformell opplæring er det som foregår ut i avdelingene en vanlig arbeidsdag. Dette innebærer samtaler og bevisstgjøring mellom kollegaer og ledelsen.

4.3.1 Formell opplæring

Ved spørsmål om virksomhetens sikkerhetsopplæring var det et klart skille mellom nyansatte og ansatte som lenge har jobbet for virksomheten. Informantene som har jobbet for virksomheten i over et år nevner kurs, samt gjennomgang av diverse dokumenter, som en del av sin formelle opplæring. I denne sammenheng blir det også nevnt å lese på relevante saker publisert på organisasjonens intranett. Disse sakene omhandler typisk nyheter innen sikkerhetsbildet, og nye trender en kan se i forhold til svindel. De ansatte mottar i tillegg e-læringsvideoer med oppdatert sikkerhetsinformasjon på e-post. Opplæring gjennom nyansattskjema og nyansattsamlinger er også rutiner som informanter med lengre arbeidsforhold har fått ta del i. Skjema og samlinger beskriver regler for bruk av eksempelvis PC, samt verdier og mål for virksomheten. En kan ut ifra våre resultater si at det på generelt grunnlag er god formell opplæring av personell med et lengre arbeidsforhold. Sikkerhetsopplæringen har derimot endret seg mye det siste året.

«Nå er vi så mange at vi ikke kan ha samtaler med hver enkelt lengre. Det har også vært kurs da, men vi er for mange til det [...] Klarer ikke følge med på hvem som starter og hvem som trenger det.» ***Informant 1***

Denne påstanden kan underbygges av samtaler med to informanter med et kortere ansettelsesforhold. Disse er begge ansatt under koronapandemien 2020. En av informantene nevner opplæring i form av kurs, der en kan oppnå sertifikat for bestått kursing. Kursene er blitt sendt over e-post, og blir av informanten beskrevet som ikke obligatoriske. I senere tid har vi forhørt oss med vår nøkkelinformant, og disse kursene har i utgangspunktet vært obligatoriske, men gjennomføringen av disse er etter koronapandemien ikke blitt fulgt opp. Det har heller ikke vært noen ytterligere informasjon eller påminnelse om at de ansatte skal gjennomføre kursene. Dette var dog den eneste form for formell opplæring informanten hadde fått siden ansettelse. Den andre av disse to informantene kan derimot ikke huske å ha hatt noen form for opplæring. Vedkommende nevner sammenhengen med korona, hjemmekontor og endring i bedriften som årsak til dette.

«Nei, var det egentlig noe sikkerhetsopplæring da? Jeg vet ikke, jeg husker i hvert fall ikke det.» ***Informant 3***

Endringen HelseIT har gjennomgått det siste året trekkes frem av flere som bakgrunn for mangelfull opplæring av nyansatte. Den formelle opplæringen ville i utgangspunktet bestått av fysiske kurs for å gi ansatte en minimumsforståelse av forventninger innen sikkerhet. Med en kraftig vekst av nyansatte er det derimot vanskelig å følge opp disse med et opplæringsopplegg som per dags dato er utdatert. HelseIT må nå i større grad benytte seg av elektroniske løsninger, men en har ikke en god nok oversikt over hvem som ansattes og hvem som har tatt kurs.

«Så vi er i en litt sånn transisjonsfase, der det sannsynligvis skal være en del ansatte akkurat nå som ikke har fått den opplæringen de skal ha rett etter de har startet.» ***Informant 2***

4.3.2 Uformell opplæring

Våre funn viser at de fleste ansatte har hatt samtaler med enten ledelsen eller kollegaer, der temaet *«sånn gjør vi det hos oss»* ble tatt opp. Da en fikk utlevert PC, ble det også gitt opplæring i form av samtaler, hvor brukerstøtteavdelingen forklarte hva en bør tenke

over ved bruk av virksomhetens utstyr. Dette mener flere er en form for uformell opplæring. Kollegaveiledning trekkes også frem som en sentral del av den uformelle opplæringen. I enkelte avdelinger er det visse sanksjonsgrep om noen eksempelvis glemmer å låse PC-skjermen. Allikevel viser våre funn at sikkerhet ikke er en naturlig del av samtalen for ansatte i flere av avdelingene.

4.4 Motivasjon

Etter en gjennomgang av våre resultater har vi valgt å kategorisere motivasjon inn i formell og uformell motivasjon. Dette da ledelsen ofte tar i bruk både formelle og uformelle virkemidler for å motivere sine ansatte til å tenke personlig sikkerhet. Med formell menes motivasjon i form av de tiltakene ledelsen gjør for å motivere de ansatte, eksempelvis publisering av artikler, videoer og annet innhold. Uformell motivasjon innebærer samtaler mellom ansatte og ledelse, samt følelsene knyttet til selve arbeidsoppgavene en gjennomfører.

4.4.1 Formell motivasjon

Da vi stilte spørsmål i forbindelse med motivasjon, var svarene i stor grad samstemte. Kursene som blir sendt via e-post, og som en får beskjed om å gjennomføre, er for informantene er stor kilde til motivasjon. Sikkerhetsmåneden i oktober blir også nevnt av flere, hvor sikkerhetsavdelingen i samarbeid med HR, deler blant annet kortfilmer, laget av Norsk senter for informasjonssikring. Basert på våre funn hva gjelder motivasjon vil vi hevde at det er stor lærevillighet blant flere av de ansatte når det kommer til sikkerhet. Sikkerhetsledere er ansatt for å skape eierskap og forankring på sikkerhetsområdene. Det er også innført et styringssystem for informasjonssikkerhet, som forklarer de grove rammene organisasjonen skal jobbe innenfor. Sikkerhetslederne skal skape innsikt i disse rammene, og motivere de ansatte til god innsats. Basert på våre funn er de formelle motiverende tiltakene mindre synlig. Resultatene viser at det i mindre grad er blitt gitt informasjon rundt sikkerhetsarbeidet under koronapandemien, og det er i mindre grad blitt fulgt opp.

4.4.2 Uformell motivasjon

Basert på våre funn kommer det tydelig frem at det er viktig for sikkerhetsledelsen å motivere de ansatte gjennom arbeidshverdagen. Dette både ved å besvare spørsmål, samt å forklare hvorfor man gjør som man gjør når det kommer til datasikkerhet. Det blir dog registrert en forskjell basert på generasjon når det kommer til motivasjon for sikkerhetsarbeid. Oppfatningen er at den yngre generasjonen har et større fokus på datasikkerhet fra før av. Våre funn viser at de fleste mener virksomheten gjør et godt arbeid med tanke på bevisstgjøring vedrørende datasikkerhet, og det stort sett ligger i bakhodet gjennom en arbeidshverdag. Våre funn viser derimot også her et skille mellom lengde på ansettelsesforhold. Det viser seg at en av våre informanter ikke har vært i samtale med noen om datasikkerhet på arbeidsplassen gjennom sine måneder som ansatt. Dette kan henge sammen med mangelfull opplæring, samt at større deler av ansettelsesforholdet har funnet sted på hjemmekontor.

> *«[…] på den tiden jeg har vært, så synes jeg ikke vi har hatt sånn super mye av det. I hvert fall ikke som jeg har bemerket meg. Vi har jo en egen sikkerhetsavdeling, men jeg har på en måte ikke så mye å forholde meg til med tanke på de da.»* ***Informant 6***

Noen av informantene trekker frem virksomhetens samfunnsansvar som en motivasjonsfaktor. Det er ekstremt viktig for HelseIT å ivareta sikkerheten, for å sikre sensitive data og andre informasjonsverdier. Enkelte opplever en frykt for å gjøre feil, og trekker også dette frem som en motivasjonsfaktor. Dette da virksomheten blant annet forvalter svært sensitiv pasientinformasjon, hvor én feil potensielt kan føre til fare for nasjonal helseberedskap.

> *«Så har det jo vært noen skremselsskudd ut der også, så en føler at man må lære seg da i tilfelle det skjer noe.»* ***Informant 3***

Våre funn viser til kommunikasjon som et middel for å skape motivasjon fra ledelsen og ut til de ansatte. Flere informanter mener det er viktig å skape en forståelse rundt

virksomhetens formål, samt engasjement for sikkerhet ved å i større grad prate med kollegaer om *«hvorfor»*, og i mindre grad om *«hvordan»*.

4.5 Organisasjonens sikkerhetskultur

Organisasjonens sikkerhetskultur oppfattes ulikt basert på arbeidsforholdets varighet. Informantene som har jobbet i HelseIT i minst et år har et noe mer positivt syn på virksomhetens sikkerhetskultur, enn de med kortere arbeidsforhold. Vi registrerer at informantene med et lengere arbeidsforhold beskriver sikkerhetskulturen som god. Det er stor bevissthet rundt taushetserklæring og hva en kan prate høyt om og ikke. For disse informantene er det et stort fokus på sikkerhet, og de er kritiske til brudd på sikkerhetsregler. Kulturen har i stor grad oppstått over tid, og en har hatt bevissthet rundt å ansette personer med gode holdninger til sikkerhet generelt. Under en ekstern-intern-revisjon for et år siden viste det seg at 95% av respondentene tenkte på sikkerhet i hverdagen.

> *«Men vi er jo en veldig sånn sikkerhetsorientert organisasjon. Alle har det ganske langt fram i pannebrasken at vi skal være sikre.»* ***Informant 1***

Våre funn viser en tydelig forskjell mellom informantenes opplevelse av sikkerhetskultur, og en møter blandede holdninger til sikkerhet basert på hvor i virksomheten en er. Overordnet sett er det gode holdninger til sikkerhet, men ved innføring av økt sikkerhet vil det i noen fagområder bli møtt med motstand. Denne motstanden oppstår trolig på grunn av en endring, og ikke nødvendigvis arbeidet med økt sikkerhet. Én nyansatt er derimot relativt usikker rundt begrepene sikkerhet og sikkerhetskultur. Resultatene våre viser lite bevissthet rundt hva som er viktig når det kommer til datasikkerhet på et personlig nivå. Trolig er dette på grunn av mangelfull opplæring, og færre motiverende tiltak mens de ansatte sitter på hjemmekontor. Sikkerhetskulturen blir beskrevet som «*sikkert fin*», som tyder på at denne ansatte ikke har samme inntrykk som de med lengere erfaring.

5 Diskusjon

I dette delkapittelet vil vi diskutere våre resultater opp mot teori. Formålet med denne delen er å danne et grunnlag for å besvare oppgavens problemstilling. Delkapittelet er inndelt i fem underkategorier, på samme vis som resultatdelen i kapittel 4.

5.1 Dagens sikkerhetsinstruks

Virksomhetens nåværende sikkerhetsinstruks er svært generisk, og fremmer ikke verdiene HelseIT ønsker å formidle. HelseIT ønsker å formidle viktigheten av sikkerhetsarbeidet, og deres påvirkning til samfunnet. Dagens instruks fremmer derimot ikke disse tingene. Den fungerer som en formalitet, og lister opp punkter som blir ansett som viktige. Basert på våre resultater er det først etter en har gjennomgått kurs de ansatte forstår viktigheten av sikkerhetsarbeidet. Den kognitive forventningsteorien sier begrepene valens, forventning og instrumentalitet henger sammen for å skape motivasjon (Einarsen & Martinsen, 2019, s. 96). Det er tydelig at de ansatte ikke ser den valensen sikkerhetsinstruksen muligens burde gi, og kanskje spesielt siden sikkerhetsopplæringen er mangelfull. Valens i dette tilfellet vil være økt sikkerhet i HelseIT. Dersom en ikke forstår formålet med instruksen, og sikkerhetsarbeidet i seg selv, blir det vanskelig å jobbe målrettet mot god datasikkerhet. Dette kan være betydningsfullt for sikkerhetskulturen til HelseIT.

Ut ifra våre funn er det ingen som husker hva sikkerhetsinstruksen inneholder. Dette kan tyde på at dens struktur og innhold ikke er av beste løsning. Siden instruksen blir sendt via elektroniske kanaler, kan mottakeren være selektiv i forhold til hva en velger å lese (Karlsen, 2018, s. 255). Da dokumentet samtidig ikke fremmer det viktigste i arbeidshverdagen, vil det kunne være vanskelig å relatere seg til innholdet. Dette kan medføre glemt innhold, noe samtlige informanter beskriver. Siden dokumentet blir fremmet som en formalitet, vil det også kunne føles som ren formalitet da en leser, og signerer. Dette kan føre til at den ikke blir ansett som noe en må tenke på aktivt i hverdagen. Dagens trusselbilde er samtidig i stadig endring (Nasjonal sikkerhetsmyndighet, 2021), noe det ikke er blitt tatt hensyn til. Instruksen har ikke blitt revidert på flere år, og den gjenspeiler derfor ikke det trusselbilde som er i dag.

Instruksen informerer derimot om noen svært sentrale elementer som er viktig for enhver ansatt, men de blir noe bortgjemt i mengden punkter.

Indirekte ledelse handler om hvordan en påvirker ansattes atferd uten direkte samhandlinger (Jacobsen & Thorsvik, 2016, s. 417). Før koronapandemien, og sammenslåingen i 2020, ble det benyttet flere opplæringsmetoder for å forbedre sikkerhetsarbeidet til de ansatte. I dag er fysisk kursing og oppfølging krevende, og store deler av de nyansattes grunnlag for sikkerhet kommer av sikkerhetsinstruksen. Det vil i en tid som denne være spesielt viktig å fremme formål og visjon gjennom instruksen, da de andre elementene for dette har falt noe bort.

5.2 Sikkerhet på personlig nivå under koronapandemien

Av våre funn tyder det ikke på at sikkerheten på et organisatorisk og teknisk nivå er endret i betydelig grad etter koronapandemien. Det fremkommer derimot at sikkerhetsfokuset på det personlige nivået har blitt svekket mens de ansatte har vært på hjemmekontor. Samtidig melder Nasjonal sikkerhetsmyndighet (2021) at pandemien har medført nye sårbarheter i dagens virksomheter. Store deler av HelseIT sitter på hjemmekontor, og nye løsninger og rutiner har blitt utviklet som en konsekvens av dette. Eksempelvis er direktørsvindel en sårbarhet som i større grad har vokst frem under pandemien (Politidirektoratet, 2021, s. 24). Denne sårbarheten blir ikke nevnt i dagens sikkerhetsinstruks, og det kan derfor være vanskelig for nyansatte å avdekke det. Ansatte som har vært en del av organisasjonen i lang tid vil ha fått informasjon om dette via kurs, intranett og nyansattsamlinger. Det fremkommer derimot at det har vært lite tilleggsinformasjon om personlig sikkerhet i den tiden tiltaket om hjemmekontor har vært innført. Dette kan tyde på at informasjon rundt dagens trusselbilde ikke er blitt formidlet, og det vil muligens være flere ansatte som ikke har et fokus på nettopp dette. Dette kan være kritisk for HelseIT dersom det ikke blir tatt tak i.

5.3 Sikkerhetsopplæring

Våre funn tyder på lite fokus hva gjelder sikkerhetsopplæring av nyansatte i virksomheten. For HelseIT har mangelfull opplæring oppstått da virksomheten har vært igjennom en omfattende endringsprosess, med ytre påvirkninger fra koronapandemien.

Kurs med fysisk oppmøte er uteblitt, og det er lite oversikt over hvilke ansatte som har gjennomført de ulike digitale kursene. Dette har ført til mangelfull opplæring av nyansatte, samt mangel på oppfølging av allerede ansatt personell. Opplæring kan på mange måter være krevende for en virksomhet der de ansatte befinner seg på hjemmekontor. Allikevel legger dagens informasjons- og kommunikasjonsteknologi til rette for effektiv ledelse der ansatte er geografisk atskilte (Kaufmann & Kaufmann, 2014, s. 236). Våre resultater viser derimot at den formelle indirekte ledelsen, som er den form for ledelse hvor en bruker elementer som eksempelvis opplæring (Jacobsen & Thorsvik, 2016, s. 417), på mange måter faller bort. Dette da en i mindre grad enn før har muligheten til å avholde kurs for å sikre god formell opplæring. Siden de ansatte samtidig sitter på hjemmekontor, vil en heller ikke ha noen naturlig form for sosialisering med andre ansatte. Dermed utgår også den uformelle opplæringen. Det blir i mindre grad mulig å hjelpe hverandre, fordi en sitter atskilt. Av våre resultater ser vi at kollegaveiledning har vært en god kilde for å sikre uformell opplæring tidligere. Dette er naturligvis vanskeligere når de ansatte sitter i hvert sitt hjem, og kommuniserer via internett. For å bedre sikkerhetsopplæringen vil det dermed være spesielt viktig å drive direkte ledelse der en kontinuerlig kommuniserer med de ansatte, og da spesielt nyansatte. Det er for de nyansatte registrert lite sikkerhetsopplæring, og dette kan være et sårbart punkt for HelseIT.

Som nevnt over gjør kommunikasjonsteknologi det mulig å benytte seg av elektroniske kanaler hvor en kan dele informasjon raskt til flere samtidig. Allikevel gir disse kanalene rom for mistolkning, samt at de mangler evnen til å formidle rik nok informasjon (Jacobsen & Thorsvik, 2016, s. 287). Dette bidrar til utfordringer ved direkte ledelse i virksomheten. En kan derimot gjennomføre digitale seminarer, hvor en fremmer datasikkerhet. Elektroniske kanaler har den fordelen av at en kan samle mange uavhengig av sted, og det kan være et effektivt verktøy for å oppdatere de ansatte om dagens trusselbilde. Dersom seminarene holdes for én og en avdeling, kan informasjonen som gis være tilpasset de ulike ansatte. På denne måten vil en kunne føle en større grad av viktighet, fordi en kjenner seg igjen i hendelsene som beskrives.

Så vel som ledelse, vil kommunikasjon være en sentral del av de ansattes uformelle sikkerhetsopplæring. Våre resultater viser til at det er lite snakk om sikkerhet på

arbeidsplassen både mellom de ansatte, og fra ledelsen. Sikkerhet på arbeidsplassen er en prinsipiell del av de ansattes arbeidshverdag, men basert på våre undersøkelser har ikke de nyansatte dette inntrykket. Da HelseIT drifter og forvalter samfunnskritiske systemer er sikkerhet noe alle må forholde seg til. Dette til tross for hjemmekontor. Det vil derimot kunne være vanskelig for nyansatte, da en ikke er blitt en del av virksomhetens sikkerhetskultur. Dermed er kommunikasjonsprosessen (Busch, Dehlin, & Vanebo, 2010, s. 388) et godt element for utøvelse av direkte ledelse. Lederne vil i denne prosessen være sender, og de nyansatte vil være mottaker av budskapet som omhandler sikkerhet på arbeidsplassen. Ledelsen må formulere budskapet på en slik måte at en som ansatt forstår hva som skal til for å opprettholde god personlig sikkerhet. Det kan se ut til at budskapet i kommunikasjonsprosessen hos HelseIT ikke kommer godt nok fram for nyansatte. Viktigheten av personlig datasikkerhet er noe en burde kommunisere ofte, og spesielt i begynnelsen av et arbeidsforhold. Siden HelseIT er i stor vekst må en tilrettelegge, og forbedre sin kommunikasjonsprosess tett opp mot disse endringene. En må velge kanal, som på grunn av koronapandemien vil være digitale plattformer. Her blir det desto viktigere å ha et klart og tydelig budskap, som gir lite rom for mistolkning. Det kan derfor være lurt å formulere seg muntlig, men samtidig bruke skriftlige virkemidler for å forsterke budskapet. Kommunikasjonsprosessen er sentral i lederens påvirkning av de ansattes vaner og holdninger allerede fra oppstart. Tydelig og effektiv kommunikasjon kan bidra til positive samtaler mellom ledelsen og de ansatte hva gjelder sikkerhet. Dette forhindrer negative holdninger, og en kan unngå dårlige vaner som kan føre til sikkerhetsbrudd.

Det kommer fram av våre resultater at det allerede er en svært god sikkerhetskultur i virksomheten. Kollegaveiledning er en viktig årsak til gode holdninger og vaner når det gjelder personlig sikkerhet. Dessverre uteblir denne formen for uformell opplæring da de ansatte nå sitter på hjemmekontor. I fysiske lokaler er det enkelt å forhøre seg med nærmeste kollega, men det kan virke noe mer krevende i en situasjon der alt foregår digitalt. Spesielt kan dette være krevende for nyansatte, da en ikke vet nøyaktig hvem en kan forhøre seg med. Dette er også en faktor som kan påvirke den eksisterende sikkerhetskulturen i virksomheten negativt. De ansatte har derimot HelseCERT, hvor en kan sende e-post dersom en har noen spørsmål. Våre resultater viser at fysisk opplæring for alle nyansatte i liten grad er gjennomført. Virksomheten har heller ikke klart å følge

opp hvem som har tatt hvilke elektroniske kurs. Dette medfører at den eneste formen for formell opplæring har vært sikkerhetsinstruksen. Dette kan true den eksisterende sikkerhetskulturen i HelseIT. En trenger i dag nye virkemidler for å holde en oversikt over nyansatte, samt hvem som har tatt kurs og ikke. Sikkerhetsinstruksen bør samtidig være oppdatert etter trusselbildet, og fremme virksomhetens verdier. Dette kan kompensere for manglende formell opplæring.

Svekket opplæring kan medføre at ansatte ikke har et forhold til de informasjonsverdiene virksomheten har. For å sikre virksomhetens eksiterende sikkerhetskultur kan det være aktuelt for ledelsen å trekke inn Herzbergs motivasjonsfaktorer (Jacobsen & Thorsvik, 2016, s. 261), fra figur 2.4. Her kan en som leder vise annerkjennelse når ansatte opprettholder god personlig sikkerhet. Dersom en gjør arbeidet med sikkerhet til noe interessant og utfordrende, kan også dette være med på å skape motivasjon. Dette fører igjen til tilfredshet som vil påvirke holdninger og vaner blant de ansatte.

Ved svikt i formell og uformell sikkerhetsopplæring kan en god sikkerhetsinstruks fungere som et verktøy for grunnleggende sikkerhetsopplæring. Dette forutsetter derimot en instruks med godt språk, og enkle retningslinjer å forholde seg til. Formål og budskap må komme godt fram, og skal gi en essensiell forståelse for sikkerhetsbehovet i virksomheten. Dette gir virksomheten en ny kommunikasjonskanal som kan bidra til bevisstgjøring av personlig datasikkerhet. En kan med jevne mellomrom sende instruksen til alle sine ansatte, både ved endringer, men også på generelt grunnlag. På denne måten vil en til enhver tid ha et dokument med relevant og viktig informasjon lett tilgjengelig. Instruksen vil dermed i mindre grad oppfattes som en formalitet, men heller som et enkelt dokument der en raskt finner svar på det en trenger svar på. En god sikkerhetsinstruks som en jevnlig sender ut til sine ansatte vil hjelpe ledelsen å sette sikkerhet på dagsordenen, samtidig som en får et større fokus på indirekte ledelse.

5.4 Motivasjon

Det er viktig å skape engasjement og motivasjon rundt datasikkerhet for å bygge en god sikkerhetskultur. Kommunikasjon er et svært viktig virkemiddel som kan påvirke dette. Det blir viktig for ledelsen å skape effektiv kommunikasjon, slik at den blir forstått av mottaker (Goodman & Truss, 2006, s. 218). Kommunikasjonsprosessen forteller at det

må være en felles forståelse mellom sender og mottaker, og dette er enklere å oppnå ved ansikt-til-ansikt-kommunikasjon (Busch, Dehlin, & Vanebo, 2010, s. 388). I HelseIT er en avhengig av at alle har god personlig datasikkerhet. Virksomheten jobber med svært sensitive data, og har en samfunnskritisk rolle i Norge. Budskapet i en sikkerhetsinstruks bør gjentas ofte, og gjerne via forskjellige kanaler, for at det skal bli oppfattet som effektiv kommunikasjon. Et gjentagende budskap vil kunne være med på å skape holdninger for sikkerhet. For å sikre at budskapet blir forstått av mottaker, kan det være en fordel å publisere utdrag fra eksempelvis sikkerhetsinstruksen, eller korte informasjonsvideoer som underbygger dens innhold. På denne måten vil en få variert informasjon i små mengder. Dette kan på mange måter være effektivt for HelseIT, da de ansatte synes det er noe mer krevende å lese igjennom dokumenter.

Av våre funn er det betydelig mindre motivasjon når det kommer til egen datasikkerhet på hjemmekontor. Det oppfattes av mange som mindre viktig, da en gjerne befinner seg alene. Årsaken til dette kan blant annet være mangelfull direkte ledelse (Jacobsen & Thorsvik, 2016, s. 417). Vi registrerer at det er blitt snakket svært lite om datasikkerhet etter en begynte å jobbe hjemmefra. Den indirekte ledelsen må i større grad gjennomføres for å motivere de ansatte, da konsekvensene av dårlig sikkerhet i verste fall kan medføre økt fare for menneskers liv og helse. Trusselbildet er i endring (Nasjonal sikkerhetsmyndighet, 2021), og de ansatte er avhengig av å holde seg oppdatert på dette. Det kan være krevende å bedrive ledelse i virtuelle organisasjoner, slik som HelseIT på flere områder defineres som etter koronapandemien. Den største utfordringen for kommunikasjonen i slike organisasjoner er fysisk avstand, i tillegg til den manglende ansikt-til-ansikt-kommunikasjonen. I verste fall kan dette medføre sosial fragmentering, noe som kan påvirke virksomhetens organisasjonskultur i negativ retning (Einarsen & Martinsen, 2019, s. 247;248). HelseIT har allikevel et godt grunnlag fra tiden før hjemmekontor, hvor ansatte allerede kjenner hverandre godt. Funnene våre viser at flere har et positivt syn på virksomhetens sikkerhetskultur. Nyansatte vil derimot potensielt kunne ha en mindre grad av tilhørighet. En kjenner ikke kollegaene sine på samme vis, og en vil kunne slite med å komme inn i den kulturen andre kjenner til. Siden starten av 2020 har det kommet mange nyansatte til HelseIT, og de utgjør en stor del av virksomheten. Dersom mange av disse ikke er blitt integrert i organisasjonskulturen, vil dette kunne medføre svekket sikkerhetskultur innad i virksomheten.

Å spre motivasjon er en viktig nøkkelfaktor for å utvikle gode holdninger (Lai, 2017) for datasikkerhet. Dersom en i liten grad snakker om sikkerhet, vil konsekvensen være mindre motivasjon. Dette viser våre funn, da fokuset har blitt svekket etter hjemmekontorløsningen. Området oppfattes ikke som like viktig, og en kan miste følelsen av sårbarhetenes alvor. Da det samtidig ikke blir formidlet av ledelsen, vil dette kunne forsterke svekket fokus. Dersom ledelsen ikke fremmer viktighet, kan det forsterke holdningene om at datasikkerhet ikke er like aktuelt. I dette tilfellet mister en ifølge den kognitive forventningsteorien både grad av valens (Einarsen & Martinsen, 2019, s. 96), forventning og instrumentalitet (Kaufmann & Kaufmann, 2014, s. 98). Valensen ved godt sikkerhetsarbeid vil være økt sikkerhet i HelseIT. Det er derimot vesentlig at dette er noe en ansatt selv ønsker. Dersom en ikke kjenner alvoret, vil ikke dette være en valens en ønsker. Forventningen ved godt sikkerhetsarbeid er at ens egne vaner, rutiner og holdninger er med på å øke sikkerheten i HelseIT, samtidig som instrumentaliteten er troen på at dette er tilfelle. Vi registrerer at flere ansatte har mistet graden av valens, forventning og instrumentalitet. Dette fordi det er blitt mindre snakk rundt personlig datasikkerhet, samtidig som det publiseres mindre innhold rundt temaet. Ifølge teorien kan dette minske motivasjonen for sikkerhetsarbeidet.

5.5 Organisasjonens sikkerhetskultur

Basert på våre funn er HelseIT en virksomhet med god sikkerhetskultur. Dette kan forklares med selektiv rekruttering, en god sosialiseringsprosess og direkte ledelse. Vi har eksempler fra våre resultater der de ansatte utsettes for sanksjonsgrep om små sikkerhetsbrudd skulle oppstå. Dette viser til god norm når det kommer til sikkerhet på arbeidsplassen. Både ledelsen og ansatte er klar over ønsket atferd, og handler på bakgrunn av dette. For en nyansatt i HelseIT vil dette være en sentral del av hens sikkerhetsopplæring, og sosialiseringsprosess. Det er her en lærer hvordan en skal forholde seg til ulike sikkerhetsreglement i praksis. Dessverre har dette gjennom koronapandemien uteblitt, da nyansatte ikke har hatt mulighet til å jobbe fra kontoret med sine kollegaer. Samtidig har den forsvinnende sikkerhetsopplæringen vært med på dette. Med digital kultur vil normer, holdninger og atferd være vanskeligere å oppfatte enn om en hadde vært i virksomhetens egne kontorlandskap. Denne type kultur kjennetegnes ofte av å la sine ansatte gjøre det som trengs i gitte situasjoner for å øke innovasjon og effektivitet (Eswaran, Soule, & George, 2019, s. 61). Dette går ofte på

bekostning av struktur og regler. For HelseIT vil det være viktig å vektlegge struktur og regler, for å opprettholde den gode sikkerhetskulturen som allerede eksisterer. En bør i så stor grad som mulig forsøke å opprettholde ønsket atferd, selv på hjemmekontor.

Våre resultater viser manglende retningslinjer i forhold til personlig sikkerhet på hjemmekontor blant alle ansatte. De ansatte gjør i stor grad som de selv vil, og tenker i mindre grad på sikkerhet. Årsaken kan være at en føler seg tryggere i sitt eget hjem, samt at en befinner seg alene. Over tid kan dette forårsake dårlige vaner som er vanskelig å endre. Vaner dannes raskt, og bidrar til å automatisere utførselen av rutinebaserte oppgaver (Karahanna & Polites, 2012, s. 25). Vanesirkelen viser kompleksiteten til en vane, og det kan være svært krevende å endre de (Duhigg, 2016, s. 313). Når en først har utviklet en vane, er det som nevnt vanskelig å endre denne tilbake til ønsket atferd. Dette fordi en vane blir sett på som noe effektivt, og det er tidkrevende å endre dette arbeidsmønsteret. Det er derfor viktig å skape gode holdninger til sikkerhet tidlig i arbeidsforholdet. Dette kan bidra til å påvirke vanene i den retningen ledelsen selv vil, før en tilrettelegger seg dårlige vaner. Gode vaner vil være med på å opprettholde dagens sikkerhetskultur, i motsetning til dårlige vaner som vil kunne bidra til en negativ endring av denne kulturen.

Det er ikke blitt gitt noe informasjon om hvordan en skal forholde seg til datasikkerhet på hjemmekontor. Sikkerhetsinstruksen forteller heller ingenting om dette. Ved å kun ha dagens sikkerhetsinstruks som opplæringsverktøy, vil en ikke kunne få et inntrykk av hvordan virksomheten ser på datasikkerhet. Dette kan medføre at en ikke skaper de holdningene og rutinene en trenger for å opprettholde sikkerhetskulturen. Dersom retningslinjer for hjemmekontor hadde vært nedskrevet i instruksen kunne man med fordel brukt denne i større grad for å fremme virksomhetens sikkerhetskultur. Etter koronapandemien vil det være interessant å undersøke hvilke konsekvenser mangelfull informasjon har gitt. En sikkerhetsinstruks med et tydelig formål og klart budskap, kan være et nyttig virkemiddel for å bedre virksomhetens indirekte ledelse. Instruksen kan bidra til å forme de ansattes holdninger og vaner til sikkerhet, både på hjemmekontor, men også fysisk i deres lokaler.

HelseIT har som nevnt gjennomgått flere, store endringer fra 2020 og til i dag. Samtidig har koronapandemien medført endringer, da store deler av virksomheten var nødt til å jobbe hjemmefra. En måtte tilpasse seg situasjonen svært raskt, og endre arbeidsprosessene slik at de også kunne utføre disse virtuelt. Abraham Maslow presenterer mangelbehov og vekstbehov i sin motivasjonsteori (Einarsen & Martinsen, 2019, s. 89). Et mangelbehov det kan være vanskelig å dekke under pandemien er det sosiale behovet. Da en jobber hjemmefra, og kun møter enkelte kollegaer virtuelt, vil en kunne miste følelsen av tilhørighet. Dette presenterer Herzberg i sin tofaktorteori som hygienefaktorer, og vil være med på å skape mistrivsel da de ikke er til stede (Jacobsen & Thorsvik, 2016, s. 261). For spesielt nyansatte vil dette kunne være et problem, da de ikke har skapt trygge, sosiale rammer på arbeidsplassen før en ble satt på hjemmekontor. Dette kan medføre et skille mellom sikkerhetskulturen før og etter pandemien. Dersom dette skillet blir for stort, vil det være krevende å gjennomgå endringen til fysiske lokaler, da endring av kultur er svært tidkrevende. Da nyansatte i dag omtrent bare har sikkerhetsinstruksen som grunnlag for hvordan en skal bevare god datasikkerhet, vil det kunne bli ekstra vanskelig å veilede disse inn i riktig vanemønster. Dette fordi instruksen som nevnt ikke inneholder retningslinjer for hjemmekontor, eller er oppdatert etter dagens trusselbilde.

Herzberg presenterer samtidig de medmenneskelige forholdene mellom overordnede og underordnede som hygienefaktorer (Jacobsen & Thorsvik, 2016, s. 261). Virtuelt arbeid kan resultere i anonyme ansatte, noe som kan være med på å svekke maktforholdet mellom overordnede og underordnede. Samtidig ser man resultater der en gjerne yter og bidrar mindre virtuelt, enn ved fysisk tilstedeværelse (Einarsen & Martinsen, 2019, s. 241;248). Når en mister de mellommenneskelige forholdene i organisasjonen, vil dette være med på å skape mistrivsel. Det er heller ingen selvfølge at en har en godt tilrettelagt arbeidsplass hjemme. Dårlige arbeidsforhold vil også være med på å skape mistrivsel ifølge Herzberg (Jacobsen & Thorsvik, 2016, s. 261). Alle disse faktorene vil kunne påvirke virksomhetens organisasjons- og sikkerhetskultur i negativ retning etter koronapandemien.

Av våre funn viser derimot også deler av arbeidshverdagen som medfører trivsel. HelseIT har et viktig samfunnsansvar, og vi registrerer en bevissthet rundt dette. Interessante

arbeidsoppgaver er en sentral faktor som medfører trivsel (Jacobsen & Thorsvik, 2016, s. 261). Disse blir av Maslow definert som vekstbehov, hvor en har gode forutsetninger for å realisere sitt eget potensiale (Kaufmann & Kaufmann, 2014, s. 95). Det kan derimot bli vanskelig i en tid med mye uforutsigbarhet, som koronapandemien medfører. Ofte blir negative sider i større grad vektlagt mer enn positive, og det vil dermed være vesentlig for HelseIT og i størst mulig grad minske faktorene som kan føre til mistrivsel.

John Kotter (2021) presenterer i sin modell åtte fokusområder en leder bør ha når en skal gjennomføre en endring med minst mulig motstand. Ved koronapandemien hadde en ikke noe annet valg enn å godta hjemmekontorløsningen, men det er viktig for ledelsen å tenke på hvilke konsekvenser dette kan ha i senere tid. Én ting er å tilpasse seg hjemmekontorløsningen, men en annen ting vil være å få HelseIT tilbake dit en var før koronapandemien. Våre funn viser nyutviklede rutiner og holdninger til datasikkerhet på hjemmekontor, noe som potensielt kan påvirke sikkerhetskulturen i senere tid. For å fremme ønskelige holdninger til sikkerhet, kan en benytte seg av John Kotter sin modell for endringsprosesser. Desto tidligere en går inn for å veilede vanene inn på riktig spor, desto enklere vil potensielt tiden etter koronapandemien være. Det vil derfor kunne være viktig å se på dette arbeidet før tilbakegangen til fysiske lokaler. Å tydeliggjøre hvilke sikkerhetsrutiner en ønsker seg, fremme budskapet om hvorfor det er viktig, samt skape forbilder og ha et tydelig fokus rundt personlig datasikkerhet vil kunne være viktig for å opprettholde en god sikkerhetskultur i virksomheten. Ved å holde et stort fokus på sikkerhet over en lengre tidsperiode, vil en kunne endre vaner og holdninger ifølge modellen. Det er derimot vesentlig for HelseIT å vite at en endringsprosess ikke kan bli ansett som vellykket før alle vaner og rutiner gir ønsket atferd. Forankringsarbeidet i ettertid, for å utvikle den sikkerhetskulturen en ønsker, er derfor vesentlig for at endringen skal bli sett på som vellykket.

5.6 Kritisk refleksjon

I delkapittel 3.5 presenterte vi Malterud (2003), referert i Berntsen (2019) fire hovedkrav til vitenskapelighet. I dette delkapittelet vil vi sette vår forskning opp mot hovedkravene, for å sikre at forskningen er av god kvalitet.

1. *Systematisk kritisk refleksjon*

Det første kravet handlet om hvorvidt våre funn var gjenbrukbare eller ikke. Oppgaven baserer seg på kvalitativ forskning, og med casestudie som hoveddesign vil det være vanskelig å oppnå overførbarhet. Dette fordi vår oppgave er sterkt avhengig av gitt kontekst. For vår casebedrift vil graden av overførbarhet være god, da våre funn kan overføres til videre forskning på temaet.

2. *Relevans*

Kravet om relevans ser på hva innhentet kunnskap kan brukes til. Vårt ønske var å innhente kunnskap som casebedriften i ettertid kunne dra nytte av. Casestudie er originalt da vår casebedrift ikke tidligere har gjennomført forskning på benyttelse av hjemmekontor under koronapandemien. Dermed vil vår problemstilling bidra til nye og unike svar for virksomheten. I tillegg vil en tilegne seg ny kunnskap i arbeidet med bacheloroppgaven.

3. *Validitet – gyldighet og pålitelighet*

Validitet sier noe om hva en faktisk har kommet fram til, og om dette er logisk og riktig i forhold til konteksten. Våre intervjuer er blitt transkribert, analysert og satt opp mot hverandre, og våre resultater er derfor logisk korrekt. Intervjuene var i tillegg formulert på en slik måte at det var vanskelig for informantene å misforstå spørsmålene. Dermed er resultatene korrekt i forhold til konteksten. Spørsmålene vi stilte hadde en klar sammenheng med problemstillingen, og alle informantene ble spurt om det samme. Resultatene har derfor en klar sammenheng.

4. *Refleksivitet*

Det siste kravet handlet om hvordan forskningsprosessen har preget oppgavens analyse og konklusjon, ved faktorer som subjektivitet, skjevhet og fordomsfullhet. Vi hadde ingen tilknytning til casebedriften før prosjektet startet, noe som er positivt da vi undersøkte et fenomen utenfra. Vårt resultat vil med dette ikke være preget av faktorer som tilhørighet og tilknytning. I forhold til informantene er disse blitt anonymisert, noe som ble presisert både av samtykkeerklæringen (Vedlegg 2), og før opptaket av intervjuet startet. Dette er med på å øke funnenes troverdighet ved å i liten grad være preget av skjevhet. Allikevel er datasikkerhet et sensitivt tema for mange, og det vil alltid være en risiko at svarene til informantene ikke er helt troverdig.

6 Konklusjon

I dette kapitelet besvarer vi vår problemstilling «*Hvordan kan en sikkerhetsinstruks påvirke en organisasjon i endring under koronapandemien?*».

På bakgrunn av en omfattende endringsprosess i 2020, med ytre påvirkninger av koronapandemien, er ikke sikkerhetsopplæringen hos HelseIT tilstrekkelig. De som i dag jobber med opplæring knyttet til informasjonssikkerhet har ikke full oversikt over hvem som er ansatt, og da heller ingen oversikt over hvem som har gjennomgått hvilken opplæring. Dette, i kombinasjon med stor vekst, har medført at flere nyansatte ikke har fått den sikkerhetsopplæringen de behøver. Sikkerhetsinstruksen utgjør derfor store deler av grunnlaget nyansatte har for å utøve god datasikkerhet, og forståelsen av hva informasjonssikkerhet innebærer. Samtidig er ikke dagens sikkerhetsinstruks oppdatert etter dagens trusselbilde. Den er ikke strukturert godt nok, og blir av de ansatte sett på som generell og formell. Den tar ikke hensyn til de aller viktigste punktene en som ansatt bør være klar over, noe som medfører at en ikke aktivt husker innholdet i arbeidshverdagen. Da sikkerhetsinstruksen fremstår som generisk, er det vanskelig å forstå hvordan en skal forholde seg til alt i praksis. Da dens budskap samtidig ikke gjenspeiler hva virksomheten i dag fremmer ved andre verktøy, forsterker dette opplevelsen om at sikkerhetsinstruksen kun er en formalitet.

Som følge av koronapandemien ble en betydelig andel av HelseIT satt på hjemmekontor. Sikkerhetskulturen i virksomheten er allerede god, men baserer seg i stor grad på kollegaveiledning. Da en nå samhandler digitalt med geografisk avstand, blir denne formen for uformell opplæring minsket. Datasikkerhet på et personlig nivå er generelt dårligere på hjemmekontor, enn i de fysiske lokalene. Temaet blir derfor ikke et naturlig samtaleemne mellom de ansatte. For de nyansatte er det derfor vanskelig å bli en del av sikkerhetskulturen virksomheten hadde før koronapandemien. Hjemmekontor medfører en mindre grad av tilhørighet, og i kombinasjon med lite direkte og indirekte ledelse, samt en mangelfull sikkerhetsinstruks, er det en fare for at ansatte utarbeider egne vaner for hvordan en håndterer datasikkerhet.

Sikkerhetskulturen står på mange måter i fare for å bli dårligere etter koronapandemien. Både på grunn av mangelfull opplæring, lite kommunikasjon rundt dagens trusselbilde

og virksomhetenes sikkerhetsinstruks. Situasjonen med hjemmekontorløsning var i utgangspunktet midlertidig, men blir stadig forlenget. Dette medfører at en som ansatt faller inn i et mønster hvor en ikke aktivt tenker på sikkerhet i den grad en gjorde fysisk på kontoret. Dagens sikkerhetsinstruks inneholder mangelfull informasjon om hvordan en skal forholde seg til sikkerhet på hjemmekontor. Dette kan være en årsak for nyutviklede vaner og rutiner på hjemmekontor. Da sikkerhetsinstruksen ikke spesifikt nevner temaet, samtidig som det ikke er blitt gitt ytterligere informasjon, kan dette ha betydning for at de ansatte ikke tenker på datasikkerhet i like stor grad som tidligere. Desto lenger situasjonen vedvarer, desto mer automatiseres vanene. Det betyr at de vil være vanskeligere å endre tilbake til akseptert atferd. For HelseIT vil det være nødvendig å allerede nå starte arbeidet med å få tilbake de sikkerhetsrutinene en ønsker.

Sikkerhetsinstruksen må være tilstrekkelig tilrettelagt for at ansatte skal kunne jobbe utenfor fysiske lokaler. Den bør revideres i henhold til trusselbildet, da dette kontinuerlig endrer seg. Når sikkerhetsinstruksen revideres bør den sendes ut til alle ansatte i HelseIT på nytt, hvor den igjen må signeres. Dette gjør at ledelsen har et klart bilde over hvilken informasjon de ansatte har mottatt, men også at ansatte er oppdatert på de sårbarhetene som eksisterer. Ved eventuelle personalsaker, vil ledelsen kun ha én instruks å forholde seg til. En vet dermed at alle i HelseIT har signert på den samme, og nyeste, informasjonen til enhver tid. Dette gjør det enklere for ledelsen å henvise til instruksen ved eventuelle sikkerhetsbrudd. For de ansatte vil det være viktig med tilgjengeliggjøring av sikkerhetsinstruksen. Dersom en er usikker på en gitt situasjon, har en noe en kan gå tilbake til dersom instruksen ligger tydelig på intranett. Samtidig bør budskapet gjentas ofte, i ulike kanaler, for å forsterke bevisstgjøringen av datasikkerhet.

For HelseIT kan en lite oppdatert sikkerhetsinstruks, mangelfull sikkerhetsopplæring, samt lite direkte ledelse ha påvirket virksomheten i negativ retning. Den generelle sikkerheten i virksomheten vil kunne være svekket da de ansatte har utarbeidet egne vaner, som en tar med seg tilbake til de fysiske lokalene. Dette kan bidra til en splittet kultur, hvor noen opprettholder god sikkerhet, mens andre i mindre grad gjør det. Dette betyr at sikkerhetsinstruksen kan ha påvirket virksomhetens sikkerhetskultur i negativ retning under koronapandemien, da den fremstår som utdatert.

6.1 Videre forskning for Casebedriften

Koronapandemien er ikke over per dags dato. Det vil derfor ikke være mulig å konkludere *hvordan* virksomheten har blitt påvirket på bakgrunn av deres sikkerhetsinstruks. Vår konklusjon er basert på funn gitt av informantene, og det tyder på at sikkerhetskulturen kan ha blitt svekket. Allikevel finnes det ingen data som bekrefter at nye vaner og rutiner vil bli tatt med tilbake til fysiske lokaler. Det vil derfor være interessant for videre forskning å gjennomføre den samme ekstern-intern-revisjonen fra 2020 etter koronapandemien. Videre vil det være relevant for HelseIT å sammenligne tidligere resultater med nye. For HelseIT vil vi allikevel anbefale å oppdatere sikkerhetsinstruksen så tidlig som mulig, for å ta hensyn til det oppdaterte trusselbildet.

6.2 Refleksjon rundt oppgavens begrensninger

Siden en sikkerhetsinstruks er individuell for hver virksomhet, er det vanskelig å konkludere på et generelt grunnlag hvilken betydning denne har. Det er flere faktorer som påvirker vår konklusjon for HelseIT, blant annet mangelfull opplæring. Allikevel vil det være aktuelt for andre samfunnskritiske organisasjoner å undersøke ettervirkningene av koronapandemien og hjemmekontorløsningen. Dette for å kartlegge hvorvidt sikkerhetskulturen og de ansattes datasikkerhet er på det samme nivået som det var før koronapandemien.

Vår bacheloroppgave retter et søkelys mot at hjemmekontor kan ha vært negativt for sikkerhetskulturen til virksomheter med sensitiv informasjon i sine systemer. Dette uavhengig om sikkerhetsinstruksen er oppdatert etter dagens trusselbilde eller ikke. Vår forskning vil derfor kunne være relevant, selv om casestudie som metode avhenger av at en forstår oppgavens kontekst.

7 Epilog

I avsluttende dialog med vår nøkkelinformant er det skjedd flere endringer i HelseIT etter vi startet med vår forskningsprosess. En har i større grad blitt bevisst over at omtrent 200 nye ansatte ikke har fått tatt del i virksomhetens organisasjons- og sikkerhetskultur. De har med dette tatt grep, og gjort en rekke tiltak for dette. Sikkerhetsinstruksen er gjennom våren 2021 blitt revidert i henhold til trusselbildet og hjemmekontor. HelseIT har samtidig gjennomført et digitalt opplæringsprogram, og hatt digitale møter som har omhandlet datasikkerhet. Virksomheten har også innført sikkerhetslunsj en gang i måneden, hvor det har vært godt oppmøte. Sikkerhetsdirektøren er bevisst på at hjemmekontor er kommet for å bli, og at en må tilpasse seg denne hverdagen. Endringene er blant annet et resultat av vår bacheloroppgave.

8 Referanseliste

Allott, N. (2019, mai). *Store norske leksikon*. Hentet april 2021 fra https://snl.no/kommunikasjon

Andersen, G. (2020, april). *Kvalitative intervjuundersøkelser*. Hentet februar 2021 fra Nasjonal digital læringsarena: https://ndla.no/nb/subject:5e750140-7d01-4b52-88ec-1daa007eeab3/topic:a317f589-7995-43aa-8b68-92182c0b23c6/topic:35efa357-acc7-4828-b241-cad5467d1dc6/resource:201ce19e-7011-49a6-b415-91fd42d5dfe9?filters=urn:filter:470720f9-6b03-40cb-ab58-e3e130803578

Askheim, O. G., & Grenness, T. (2018). *Kvalitative metoder for markedsføring og organisasjonsfag* (Vol. 3). Oslo: Universitetsforlaget.

Beatty, C. A. (2015). *Communicating during an organizational change.* Kingston: Queens University.

Bergsjø, H., & Windvik, R. (2018). *Datasikkerhet for ledere.* Oslo: Universitetsforlaget.

Berntsen, K. E. (2019). *Vitenskapelig forankring av bacheloroppgaven: Del 2 (VT2).* Hentet april 2021 fra leksjon i Bacheloroppgave i Digital forretningsutvikling (IBED3001), ved NTNU.

Bolman, L. G., & Deal, T. E. (2018). *Nytt perspektiv på organisasjon og ledelse* (6. utg., Vol. 1). Oslo: Gyldendal.

Bostad, T., Røyert, H., & Paulsen, T. M. (2020, oktober). *Holdninger*. Hentet april 2021 fra ndla: https://ndla.no/subject:24/topic:1:183732/topic:b6562a48-8510-46b3-a0d2-b53dd9da349f/resource:1:25440?filters=urn:filter:777ae87e-ca79-4866-920a-115cfeb7bbe1

Busch, T. (2019). *Akademisk skriving for bachelor- og masterstudenter* (Vol. 5). Bergen: Fagbokforlaget.

Busch, T., Dehlin, E., & Vanebo, J. O. (2010). *Organisasjon og organisering* (6. utg.). Oslo: Universitetsforlaget.

Bø, O. (1995). *FOU-metodikk.* Otta: TANO AS.

Cummings, T., Worley, C., & Donovan, P. (2019). *Organization Development and Change.* London, United Kingdom: Cengage Learning EMEA.

Direktoratet for forvaltning og økonomistyring. (2020, februar). *Hva og hvorfor er det viktig?* Hentet mars 2021 fra Direktoratet for forvaltning og økonomistyring: https://dfo.no/fagomrader/etats-og-virksomhetsstyring/etatsstyring/miniveileder-om-oppfolging-av-informasjonssikkerhet-i-styringsdialogen/hva-er-informasjonssikkerhet-og-hvorfor-er-det-viktig

Duhigg, C. (2016). *Vanens makt.* Norge: Stenersens forlag.

Einarsen, S. V., & Martinsen, Ø. L. (2019). *Organisasjon og ledelse* (1. utg., Vol. 2). (A. Skogstad, Red.) Oslo: Gyldendal.

Eswaran, A., Soule, D. L., & George, W. (2019). *Building digital-ready culture in traditional organizations.* Mit Sloan Management Review.

Goodman, J., & Truss, C. (2006). *The medium and the message: communicating effectivly during a major changle initiative.* London: Journal of Change Management.

Grønmo, S. (2020a, november). *Kvalitativ metode*. Hentet februar 2021 fra Store norske leksikon: https://snl.no/kvalitativ_metode

Grønmo, S. (2020b, juni). *Kvantitativ metode*. Hentet februar 2021 fra Store norske leksikon: https://snl.no/kvantitativ_metode

Gundersen, D., Johansen, P., & Bjerkestrand, N. E. (2018, februar). *Transkripsjon*. Hentet mars 2021 fra Store norske leksikon: https://snl.no/transkripsjon

Haukdal-Brochs, W. (2011). *Arbeids- og lederpsykologi* (8. utg., Vol. 2). Oslo: Cappelen akademiske forlag.

Jacobsen, D. I. (2018). *Organisasjonsendringer og endringsledelse* (3. utg., Vol. 1). Bergen: Fagbokforlaget.
Jacobsen, D. I., & Thorsvik, J. (2016). *Hvordan organisajoner fungerer* (4. utg., Vol. 4). Bergen: Fagbokforlaget.
Jamieson, S. (2007). *Likert scale.* Hentet mai 2021 fra Britannica: https://www.britannica.com/topic/Likert-Scale
Karahanna, E., & Polites, G. L. (2012). *Shackled to the Status Quo: The Inhibiting Effects of Incumbent System Habit, Switching Costs, and Inertia on New System Acceptance.*
Karlsen, J. T. (2018). *Prosjektledelse - fra initiering til gevinstrealisering* (4. utg., Vol. 2). Oslo: Universitetsforlaget.
Kaufmann, G., & Kaufmann, A. (2014). *Psykologi i organisasjon og ledelse* (4. utg., Vol. 5). Bergen: Fagbokforlaget.
Kotter International. (2021). *8 steps process for leading change*. Hentet april 2021 fra Kotter Inc: https://www.kotterinc.com/8-steps-process-for-leading-change/
Lai, L. (2017). *Strategisk kompetanseledelse* (3. utg., Vol. 4). Bergen: Fagbokforlaget.
Mørch, W. T. (2020, juli). *Abraham Maslow*. Hentet mai 2021 fra Store norske leksikon: https://snl.no/Abraham_Maslow
Nasjonal sikkerhetsmyndighet. (2019, mars). *Hva er personellsikkerhet?* Hentet mars 2021 fra Nasjonal sikkerhetsmyndighet: https://nsm.no/fagomrader/personellsikkerhet/hva-er-personellsikkerhet-1/
Nasjonal sikkerhetsmyndighet. (2021, februar). *Et komplekst og skjerpet nasjonalt risikobilde.* Hentet mars 2021 fra Nasjonal sikkerhetsmyndighet: https://nsm.no/aktuelt/et-komplekst-og-skjerpet-nasjonalt-risikobilde
Nasjonal sikkerhetsmyndighet. (u.d.). *Grunnprinsipper for personellsikkerhet.* Hentet mars 2021 fra Nasjonal sikkerhetsmyndighet: https://nsm.no/regelverk-og-hjelp/rad-og-anbefalinger/grunnprinsipper-for-personellsikkerhet/opprettholde-og-oppdage/skape-en-god-sikkerhetskultur/
Nettvett. (2020, mai). *Håndbok for informasjonssikkerhet*. Hentet mars 2021 fra Nettvett: https://nettvett.no/handbok-for-informasjonssikkerhet/
Norsk senter for informasjonssikring. (2017, november). *Nordmenn og digital sikkerhetskultur.* Hentet mars 2021 fra Norsk senter for informasjonssikring: https://norsis.no/wp-content/uploads/2017/11/Nordmenn-og-digital-sikkerhetskultur-2017.pdf
Næringslivets Hovedorganisasjon. (2021). *Sikkerhetskultur*. Hentet april 2021 fra Arbinn: https://arbinn.nho.no/hms/sikkerhet-og-beredskap/sikkerhet/sikkerhet/sikkehetskultur/
Nätt, T. H. (2020, desember). *Informasjonssikkerhet*. Hentet mars 2021 fra Store norske leksikon: https://snl.no/informasjonssikkerhet
Patel, R., & Davidson, B. (1999). *Forskningsmetodikkens grunnlag: å planlegge, gjennomføre og rapportere en undersøkelse* (Vol. 2). Oslo: Universitetsforlaget.
Personopplysningsloven. (2018, §1). *Lov om behandling av personopplysninger (LOV-2018-06-15-38).* Lovdata. https://lovdata.no/dokument/NL/lov/2018-06-15-38/*#KAPITTEL_1.
Politidirektoratet. (2021, februar). *Politiets trusselvurdering 2021*. Hentet mars 2021 fra Politiet: https://www.politiet.no/globalassets/04-aktuelt-tall-og-fakta/politiets-trusselvurdering-ptv/2021-02-12-o-ptv-2021.pdf
Politiets sikkerhetstjeneste. (2021, februar). *Nasjonal trusselvurdering 2021.* Hentet mars 2021 fra PST: https://www.pst.no/globalassets/artikler/trusselvurderinger/nasjonal-trusselvurdering-2021/ntv_2021_final_web_1802-1.pdf

Ramlall, S. (2004). *A Review of Employee Motivation Theories and their Implications for Employee Retention within Organizations.* Cambridge: The Journal of American Academy of Business. Hentet mars 2021

Sagberg, I. (2020, august). *Frederick Herzberg*. Hentet mars 2021 fra Store norske leksikon: https://snl.no/Frederick_Herzberg

Sagberg, I. (2021, april). *Ledelse*. Hentet mai 2021 fra Store norske leksikon: https://snl.no/ledelse

Schackt, J. (2019, september). *Kultur*. Hentet mars 2021 fra Store norske leksikon: https://snl.no/kultur

Selnes, F., & Lanseng, E. J. (2014). *Markedsføringsledelse med digitale verktøy* (1. utg.). Oslo: Gyldendal Norsk Forlag.

Sundbye, L. M., & Nisted, I. M. (2017, oktober). *Primære og sekundære datakilder*. Hentet februar 2021 fra Nasjonal digital læringsarena: https://ndla.no/nb/subject:7/topic:1:183191/topic:1:105795/resource:1:93370?filters=urn:filter:433559e2-5bf4-4ba1-a592-24fa4057ec01

Svartdal, F. (2020, mai). *Sosialpsykologi*. Hentet mai 2021 fra Store norske leksikon: https://snl.no/sosialpsykologi

Sætre, A. S. (2009). *Kommunikasjon i organisasjoner.* Bergen: Fagbokforlaget.

Teigen, K. H. (2020, mars). *Motivasjon*. Hentet mars 2021 fra Store norske leksikon: https://snl.no/motivasjon

Vroom, V. H. (1994). *Work and Motivation.* San Francisco: Jossey-Bass Inc.

Vedlegg 1 – Intervjuguide

- Presentere oss selv og prosjekt og formål med datainnsamling
- Gå gjennom informasjonsskriv og innhente muntlig eller skriftlig samtykke til deltagelse, opptak og anonymisering

Tema	Spørsmål
Intro	1. Hva er din bakgrunn? 2. Hva er din stilling hos HelseIT, og hvor lenge har du jobbet her? 3. Hvilken erfaring har du med informasjonssikkerhet? Gjerne kom med eksempler fra din arbeidshverdag.
Generelle spørsmål om sikkerhet i organisasjonen	1. Hvilke tanker har du rundt personlig sikkerhet når du jobber med ulike arbeidsprosesser? For eksempel mail, hjemmekontor, sosiale medier, holdninger og vaner. 2. Er det stort fokus på personlig sikkerhet mellom ansatte, og fra ledelse? Hvordan er fokuset på hjemmekontor? 3. Hvilken type opplæring har du fått når det gjelder personlig sikkerhet? 4. Snakker ledelsen med dere om personlig sikkerhet, og viktigheten av det når dere sitter på hjemmekontor? 5. Hvordan er sikkerhetskulturen? a. Hvordan har den oppstått? b. Hva med på hjemmekontor? c. Har den evt. endret seg noe siden dere ble satt på hjemmekontor? 6. Gjør ledelsen tiltak for å motivere dere til å tenke på personlig sikkerhet? Når dere sitter på hjemmekontor? 7. Snakker ledelsen med dere om personlig sikkerhet, og viktigheten av det når dere sitter på hjemmekontor? 8. Vet du hvem du kan prate med dersom det er noe spørsmål rundt instruksen, eller sikkerhet generelt?
Spesifikke spørsmål rundt virksomhetens sikkerhetsinstruks	1. Når vi sier sikkerhetsinstruks – hva tenker du da? 2. Hvilket forhold har du til instruksen? 3. Hva oppfatter du er hovedpoenget med instruksen? 4. Forsto du innholdet, og oppfatter du den som detaljert eller overordnet? 5. Har du noen tanker rundt hvordan instruksen kan brukes annerledes? 6. Har du siden ansettelse blitt oppfordret til å lese instruksen på nytt? 7. Mener du dagens sikkerhetsinstruks fungerer som et kommunikasjonsverktøy fra ledelsen og ut til de ansatte? 8. Hvordan kan sikkerhetsinstruksen motivere deg til å tenke personlig sikkerhet?
Avslutning	1. Har du noen innspill, eller noe du vil nevne som du finner interessant eller nyttig for vår oppgave? 2. Har du tips til noen andre vi eventuelt kan ta kontakt med for å gi oss mer informasjon? 3. Takke for oss, og takke for gode bidrag til oppgaven.

Vedlegg 2 – Samtykkeskjema

Vil du delta i forskningsprosjektet *«Digital forretningsutvikling»*?

Dette er et spørsmål til deg om å delta i et forskningsprosjekt hvor formålet er å kunne studere anvendelse av IT og hvordan dette kan skape gevinster for virksomheten. I dette skrivet gir vi deg informasjon om målene for prosjektet og hva deltakelse vil innebære for deg.

Formål
Denne oppgaven er en bacheloroppgave i studiet Bachelor i Digital forretningsutvikling ved Institutt for datateknologi og informatikk NTNU, og vil forsøke å belyse et tema tilhørende den overordnede problemstillingen om hvordan anvendelse av IT på ulike måte kan skape gevinster for virksomheten.

Hvem er ansvarlig for forskningsprosjektet?
NTNU, Ragna Skjei og Marte Marjorie Søgnen er ansvarlig for prosjektet.

Hvorfor får du spørsmål om å delta?
Du har fått spørsmål om å delta fordi oppdragsgiver har anbefalt deg. All kontaktinformasjon er blitt gitt fra oppdragsgiver.

Hva innebærer det for deg å delta?
Å delta innebærer å svare på utvalgte spørsmål i et intervju, hvor tiden har blitt satt til 45 minutter. Intervjuet handler om personlig sikkerhet på arbeidsplassen, og om hvilke holdninger du har til personlig sikkerhet. Intervjuet vil skje via Microsoft Teams, og det vil bli tatt opptak.

Det er frivillig å delta
Det er frivillig å delta i prosjektet. Hvis du velger å delta, kan du når som helst trekke samtykket tilbake uten å oppgi noen grunn. Alle dine personopplysninger vil da bli slettet. Det vil ikke ha noen negative konsekvenser for deg hvis du ikke vil delta eller senere velger å trekke deg.

Ditt personvern – hvordan vi oppbevarer og bruker dine opplysninger
Vi vil bare bruke opplysningene om deg til formålene vi har fortalt om i dette skrivet. Vi behandler opplysningene konfidensielt og i samsvar med personvernregelverket.

- *Ved behandlingsansvarlig institusjon vil prosjektgruppe og veileder ha tilgang.*
- *Opptak ved intervjuer vil lagres på sikret nettverk/digital plattform der NTNU har databehandleravtale*

Hva skjer med opplysningene dine når vi avslutter forskningsprosjektet?
Opplysningene anonymiseres når prosjektet avsluttes/oppgaven er godkjent, noe som etter planen er 01.06.2021. *Personopplysninger og opptak slettes innen prosjektslutt.*

Dine rettigheter
Så lenge du kan identifiseres i datamaterialet, har du rett til:

- Innsyn i hvilke personopplysninger som er registrert om deg
- Å få utlevert en kopi av opplysningene
- Å få rettet personopplysninger om deg
- Å få slettet personopplysninger om deg
- Å sende klage til Datatilsynet om behandlingen av dine personopplysninger.

Hva gir oss rett til å behandle personopplysninger om deg?
Vi behandler opplysninger om deg basert på ditt samtykke.

På oppdrag fra NTNU har NSD – Norsk senter for forskningsdata AS vurdert at behandlingen av personopplysninger i dette prosjektet er i samsvar med personvernregelverket.

Hvor kan jeg finne ut mer?
Hvis du har spørsmål til studien, eller ønsker å benytte deg av dine rettigheter, ta kontakt med:

- NTNU ved Jostein Engesmo (jostein.engesmo@ntnu.no)
- Vårt personvernombud: Thomas Helgesen.
- NSD – Norsk senter for forskningsdata AS, på epost (personverntjenester@nsd.no) eller telefon: 55 58 21 17.

Hvis du har spørsmål knyttet til NSD sin vurdering av prosjektet, kan du ta kontakt med:

- NSD – Norsk senter for forskningsdata AS på epost (personverntjenester@nsd.no) eller på telefon: 55 58 21 17.

Med vennlig hilsen

Prosjektansvarlige
Ragna Skjei og Marte Marjorie Søgnen

Veileder
Torstein Hjelle

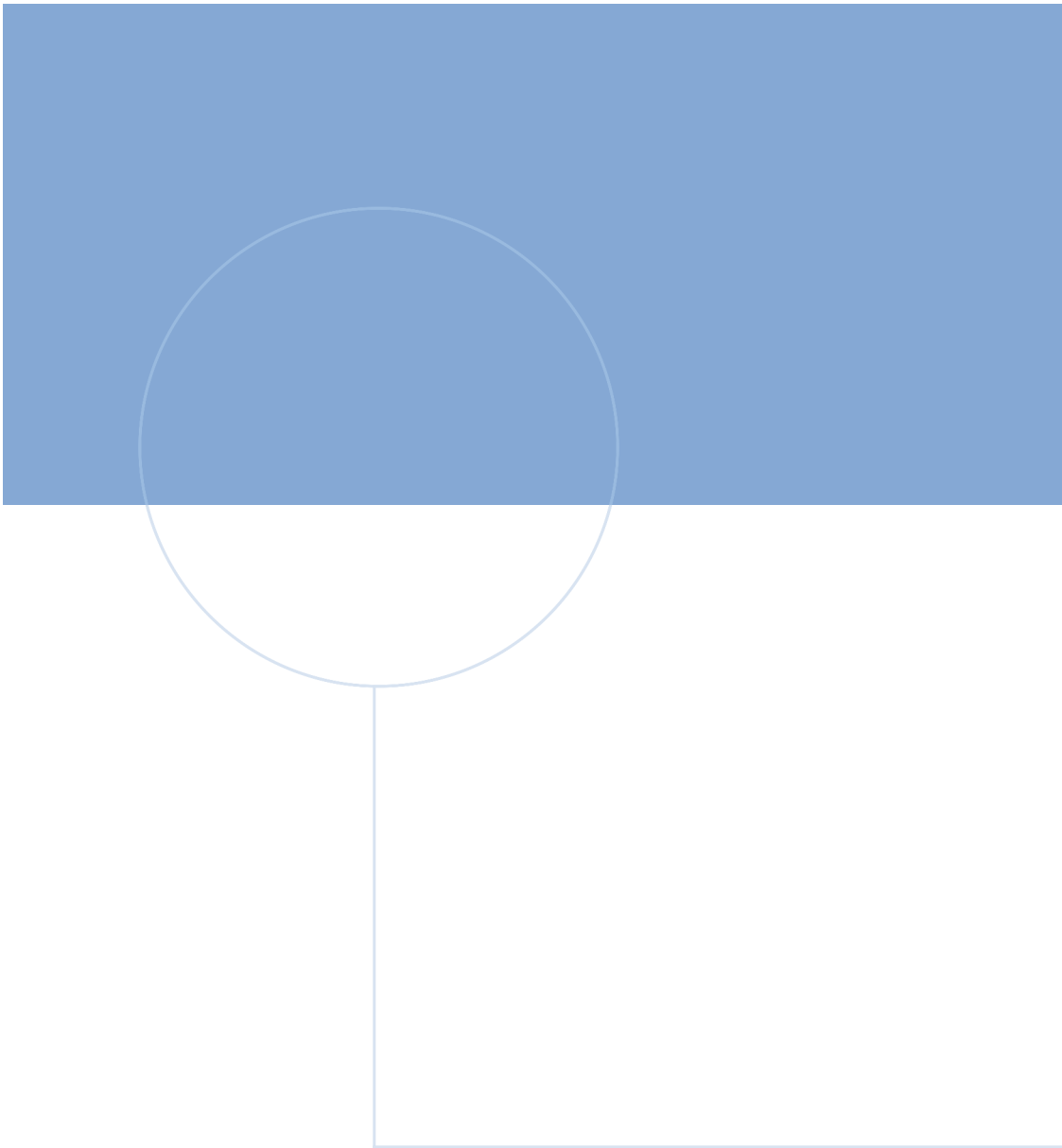
Samtykkeerklæring

Jeg har mottatt og forstått informasjon om prosjektet *Digital forretningsutvikling*, og har fått anledning til å stille spørsmål. Jeg samtykker til:

- ☐ Å delta i intervju
- ☐ At intervjuet blir tatt opp
- ☐ At opplysningene som gis under intervjuet blir anonymisert, og kan benyttes som en del av bachelorprosjektet

Jeg samtykker til at mine opplysninger behandles frem til prosjektet er avsluttet 01.06.2021

(Signert av prosjektdeltaker, dato)



NTNU

Kunnskap for en bedre verden