**Case 3: Skyggefjell Skibakker AS – Trekkoppgaver**

**16.04.2024 – 2IT**

**Sander Wettermann Rasmussen**

**Innhold**

[Del 1: Planlegging av IT-Infrastruktur 2](#_Toc164362835)

[A. Lag et logisk nettverkskart og beskriv infrastrukturen i nettverket 2](#_Toc164362836)

[B. Sikkerhetstiltak i nettverket mot uautorisert tilgang. Beskriv Personvern sikring. 7](#_Toc164362837)

[Del 2: Planlegging av App/Nettside 9](#_Toc164362838)

[A. Lag en skisse av appen og beskriv de viktigste funksjonene den vil ha 9](#_Toc164362839)

[B. Beskriv database-designet og infoen den vil lagre og hvordan den er strukturert. 13](#_Toc164362840)

[Del 3: Drøfting rundt datainnsamling og Personvern 18](#_Toc164362841)

[A. Hvilke fordeler og ulemper finnes innen innsamling av heistur data. 18](#_Toc164362842)

[Fordeler 19](#_Toc164362843)

[Ulemper 19](#_Toc164362844)

[B. Hvordan vil vi sikre at gjestene er klar over innsamlingen og sikre deres personvern 20](#_Toc164362845)

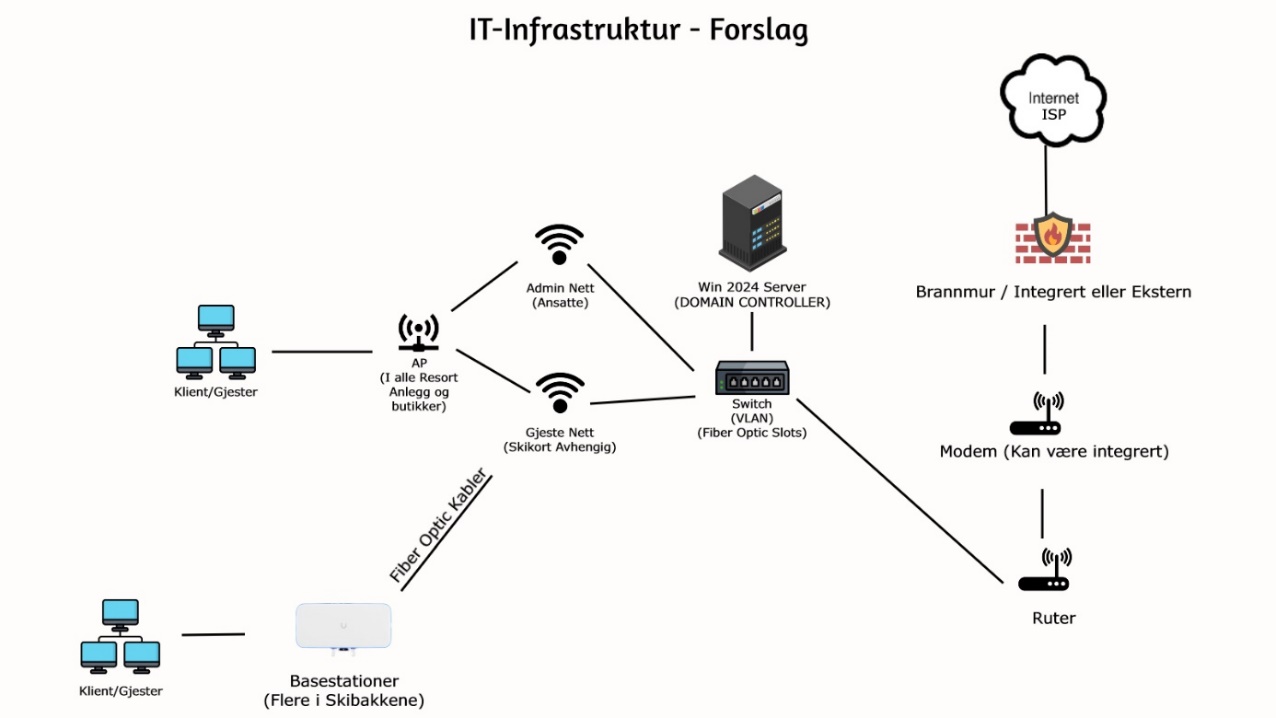
# Del 1: Planlegging av IT-Infrastruktur

## Lag et logisk nettverkskart og beskriv infrastrukturen i nettverket

Skyggefjell Skibakker AS har et ønske om å få på plass en topp kvalitets skibakke med et godt trådløst nettverk med god sikkerhet. De ønsker totalt 2 nettverk som er separert, 1 ansattnettverk og 1 gjestenettverk. Det trådløse nettverket skal være tilgjengelig over hele området & skibakkene, samt at gjestenettverket skal kun klare å bli koblet til av besøkende/beboere med aktivt skikort.

Nedenfor er et bilde over mitt hovedforslag til IT-Infrastruktur hos Skyggefjell Skibakker AS, noen deler av denne kan endre seg basert på behov og kostnad, men siden de er opptatt av å ha topp kvalitet med god kamerastrømming, samt et fokus på å omgjøre store deler av bakken er det like greit å gjøre det ordentlig når man først gjør slike endringer.

Under bildet vil du finne en litt mer detaljert oversikt over hver enhet i infrastrukturen, hva dens oppgave er og annen relevant informasjon.



* **ISP / Internett**

ISP eller også kalt Internett Service Provider, er hvor vi henter inn nettverk fra. Dette er rett og slett tilkoblingen vår til det offentlige internett gjennom vår Internettleverandør. Her er det flere standarder, men vi kommer nokk til å ha Fiber med tanke på at de ønsker høy kvalitet. Dette nettet blir dermed da sent gjennom en fiberkabel med lys inn til modemet vårt.

* **Modem**

Modemet i nettverket vårt vil hjelpe oss med å gjøre om alle digitale signaler til analoge og alle analoge til digitale, med andre ord så konverterer den signaler. Dette gjør det mulig for ruteren å ta inn lys informasjon fra fiber kabelen og lese maskinkode fra den, og gjør det mulig å sende data gjennom kabelen til internett med lys også. Modemet kan både være en egen boks, samt være integrert i ruteren.

* **Brannmur**

Brannmuren i nettverket mitt kan være både ekstern // en egen enhet, samt at vi også kan integrere den i ruteren og bruke den på et logisk plan. Brannmuren er en sikkerhets enhet for nettverket vårt og passer på at kun tillatt trafikk går inn og ut. Alt som er definert som «ikke lov», eller motsatt alt som er ikke er definert som «lov» blir filtrert ut og blokkert. Med brannmur kan man for eksempel Geo-Blokkere, man kan blokkere porter og ip-er fra aktører som er identifisert som svindel eller skadelig.

* **Ruter**

Ruteren i nettverket vil ha rollen av å opprettholde og gjennomføre flere protokoller og rett og slett rute trafikken på nettverket vårt. På Rutern finner vi blant annet protokoller som IP Protokollen, DHCP, NAT og mer. Ruteren er også hvor LAN og WAN skilles.

* **Switch**

Switchen i nettverket her kommer etter ruteren og er koblet ut mot andre enheter som aksesspunkter, basestasjoner etc. Denne switchen må ha nokk porter til å dekke alle enheter både gjennom ethernet og fiber optic kabler.

Switchen har rollen som «Aktiv Sentral». Switchen har i oppgave å sende data og informasjon til og fra enheter gjennom riktige noder i nettverket vårt. Med andre ord om du er plassert over Aksesspunkt A, er det bare den noden som blir videresendt din data og ikke alt annet. Switchen har kontroll over hvilke enheter som er tilkoblet og hvor dataen sendes.

I nettverket mitt vil jeg benytte meg at **Stjerne Topologien // Star Topologi** hvor switchen spiller en større rolle da det kommer til sending av trafikk ut til andre noder // Aksesspunkter & Basestasjoner. Grunnen til at jeg velger Stjerne Topologi er veldig enkelt: Først og fremst så er denne typen oppsett veldig populært rundt om i verden på grunnlag av dens effektivitet og simplisitet.

Ved å innføre en slik topologi er det enklere å sette opp og man mister ikke mye om 1 av nodene blir skadd / ødelagt. Er det slik at et aksesspunkt ryker kan man enkelt erstatte dette og fortsette uten at andre enheter blir påvirket, eneste negative med dette er jo at om Sentralen // Switchen blir ødelagt er nettverket og topologien nede og må settes opp igjen med ny switch, men det skal nokk gå greit så lenge man gjennomfører god og ofte vedlikehold & utstyrs sjekk.

* **Win Server**

For å kontrollere brukertilganger, rettigheter og generelt administrere brukere og passord behøver jeg å sette opp Active Directory over nettverket mitt og dens enheter. Her kommer Windows Serveren inn i bildet.

For å sette opp Active Directory trenger jeg kun en Windows Server og dens innebygde verktøy. Med AD på nettverket vil den ta av seg arbeidet som DHCP egentlig gjør på ruteren, med andre ord utdeling av IP-Adresser til de med rettigheter / konfigurerte brukerkontoer.

Her kan man for eksempel si at mennesker i gruppen «Ansatt» får tilgang til ansattnettverket med brukerinnlogging, samtidig som alle brukere i gruppen «Beboer/Gjest» får tilgang til gjestenettverket med deres email og passord.

Planen min med Serveren er å kontrollere disse tilgangene, samt benytte AD til å lage gjestebrukere for meg. Jeg kan nemlig koble opp Web Serveren til AD, slik at når noen bestiller et rom blir en AD-Bruker opprettet enten med engang, eller når de har sjekket inn, slik at jeg kan gi nett tilgang til de som faktisk har et aktivt skikort og restriktere tilgang til de uten. Her kan jeg for eksempel bruke data fra web-databasen til å sjekke når noen er sjekket inn og datoen de drar blir kontoen slettet fra AD etter ønske fra firmaet. (Trenger DNS // Domain Services og DHCP for oppsett av AD)

* **Admin & Gjestenett**

På nettverket mitt vil jeg benytte meg av noe som heter VLAN, eller også kalt «Virtual Local Area Network». Ved bruk av VLAN og Trunk kabler gjennom mine aksesspunkt kan jeg strømme flere nettverk samtidig over et sett av utstyr, som sparer kostnadene og hjelper med å separere nettverket i flere ulike deler med ulike rettigheter. Med andre ord opprette 1 Admin nett med sine egne tilganger, og 1 Gjestenett med sine.

Grunnen til at jeg gjør dette er fordi de ønsket 2 egne nettverk og derfor leverer jeg denne løsningen som er økonomisk smart og fungerende med hjelp av AD. Bemerk at jeg kan bare bruke Trunk-Kabler over aksesspunkt, ikke basestasjoner. Dermed vil basestasjonene bare ha gjestenettverk, men det skal nokk gå fint mtp at ansatte ikke arbeider på nettsidene oppe i skibakkene.

Admin nettverket vil ha tilgang til interne ressurser og eventuelt tilgang til databasen, mens Gjestenettverket vil være et åpent nettverk for alle gjester med aktivt skikort for å surfe på internett og kose seg på deres opphold. Jeg vil anbefale overvåkning av trafikken for å passe på at alt er i orden til enhver tid, men det skal nokk ikke være store problemer rundt dette.

Mitt nettverk kommer til å bruke WPA3 og AES som krypteringsmetoder, God fysisk sikring er et krav. Her snakker vi nøkkelkort, gode låser og god plassering av utstyr vekk fra kundenes/besøkendes hender. Her vil også Active Directory serveren være godt beskyttet siden den har all informasjon om alle brukere, samt at den vil være MFA beskyttet.

* **Aksesspunkt**

Aksesspunktene som jeg tar bruk av har en stor rolle i mitt nettverk. Aksesspunktene er det som gjør det mulig i mitt nettverk til å opprettholde en trådløs tilkobling, med andre ord tilgjengeliggjøre nettverket som Wi-Fi. Aksesspunktet tar seg av arbeid som SSID (Nettverksnavn), Styrer all kommunikasjon som skjer i den trådløse sonen, kryptering av datapakker og kommunikasjon, samt at det er det som er bindeleddet mellom trådløs enhet og nettverket.

Mine aksesspunkt vil være sikret med den nyeste standarden innenfor Kryptering WPA3 og vil være fysisk sikret gjennom god plassering uten god tilgang for gjester, samt kablingen til aksesspunktene vil gå gjennom vegger og tak. Dette vil forhindre både fysisk og logisk tilgang til uautoriserte brukere. Siden jeg benytter meg av flere aksesspunkter rundt om på resorten og dens anlegg, er det smarteste å kjøpe inn flere aksesspunkter og til slutt 1 nettverkskontroller som kan samle alle enhetene og enkelt la oss konfigurere alle enheter på 1 og samme gang, noe som sparer oss for tid og penger i fremtiden.

* **Basestasjoner**

Basestasjoner er noe som jeg trenger å ta innkjøp av om vi skal gjennomføre min hoved løsning. I oppgaven står det klart og tydelig at Skyggefjell Skibakker AS ønsker at nettverket skal strekke seg over alle skibakker og være tilgjengelig for alle besøkende. For å gjøre dette mulig har jeg sett **på Basestation XG fra Unifi**. Disse koster litt, men har god rekkevidde (Rundt 465m) og kan håndtere trafikken fra rundt 1500 sanntidsenheter. Nå antar jeg at bakkene kan være alt fra 400-1000+ meter lange, dermed ville jeg anbefalt å kjøpe inn flere av de og plassere taktisk rundt om i bakene hvor de både har god dekning til bakken, samtidig som de er vanskelig å både se, samt få tak i.

For å få disse til å fungere benytter vi oss av Fiber Optic kabler til vår Switch slik at vi kan opprettholde god hastighet og minimere datatap over lengre distanser som dette. Dette er litt kostbart, men veldig verdt det på langsikt. Basestasjonene fungerer akkurat likt som et Aksesspunkt, men de har bare en mye større distanse.

Andre løsninger som kunne ha blitt tatt i bruk som jeg ikke velger å anbefale som mitt førstevalg er blant annet å sette opp Basestasjoner eller long-range aksesspunkter med P2P(Point-To-Point) forbindelser. Dette reduserer antall kabler og kostnader oppe i fjellet, men reduserer nettverkskvaliteten & hastigheten, som igjen hemmer Live-Kameraene som skal streame i 4K i sanntid. P2P Kan fungere som et billigere valg enn fiber, men ytelsen vil være meget dårligere, og ikke minst enklere å påvirke da det kommer til vær og storm.

I tillegg til P2P kunne man også ha satt opp en massiv mengde med Aksesspunkter og Repeatere oppe i fjellet for å styrke signalet, men dette ville hverken vært billig eller enkelt. Da må man med andre ord holde styr på et sykt antall mengde enheter og deres konfigurasjon og status til enhver tid, istedenfor å holde styr på rundt 10, noe som er en stor forskjell. Det vil kanskje ikke koste like mye utstyrs messig, men antall arbeidstimer brukt og lønnskostnader vil være alt for høyt til at det blir vært det. Dermed er min anbefaling, i min mening, det som vil gi best oversikt, ytelse og ikke minst timer spart.

## Sikkerhetstiltak i nettverket mot uautorisert tilgang. Beskriv Personvern sikring.

Da man logger seg på alle type nettverk kan alltids angrep forekomme om de treffer riktig, men med tiltak på plass kan man redusere både sannsynligheten til at disse angrepene gjør skade, samtidig som man kan redusere skadene ved å sikre dataen som blir sendt og opprettholde høy sikkerhet innen tilgang til nettverket.

Får å starte med **kryptering av nettverkstrafikk/kommunikasjon og data**. Alle enheter som blir brukt av Skyggefjell Skibakker AS vil ta bruk av den nyeste standarden innenfor nettverkssikkerhet. Her vil vi benytte oss av WPA3 og AES kryptering på kommunikasjonen slik at alle pakker er krypterte med ulike nøkkler, vi sikrer oss mot ordbok & bruteforce angrep bedre og mer. Denne krypteringen vil sikre all data som går inn og ut på en god måte.

Videre til **tilgangskontroll**. Som nevnt i oppgaven er det bare Ansatte og Gjester som skal ha tilgang til sine respektive nettverk, noe som jeg velger å gjøre gjennom Active Directory og Web-Databasen. Her er det viktig å ta bruk av brukeradministrasjon for å forhindre at brukere som gjester får tilgang til ting kun ansatte skal ha og motsatt. Tilgangskontroll/AD vil bli brukt for å restriktere tilgang til kun de som skal ha dette, samt la oss enkelt fikse opp i bruker & konfigurasjonsfeil om noe skulle ha skjedd.

For å starte med Gjestene, alle gjester på vår resort må jo registrere og booke rom gjennom vår nettside. Her kommer vi til å informere om hvilke data vi lager og hva som skjer videre, noe som de må gi samtykke til for å bekrefte at dette er greit. Videre lagrer vi data som e-post, booking datoer og navn slik at vi kan kontakte de. Når de har bestilt sender vi de en ordrebekreftelse, samt en e-post for å lage et eget passord til «Min Side» på vår web-portal. Når de har gjort dette vil de ikke bare få en bruker på web-siden, men også en AD bruker med likt brukernavn/epost og passord. Dette vil jo såklart være **hashet** slik at man ikke kan lese hva det egentlig står der. Kun datamaskinen har **krypteringsnøkkelen** og kan sjekke, noe som ikke bare beskytter deres personvern og informasjon, men også sikrer at ingen uautoriserte brukere kan «cracke» informasjonen heller om de plutselig får tilgang på filene.

Ved bruk av AD, databaseinformasjonen og litt koding kan vi for eksempel si at når Booking datoene har ankommet blir AD-Brukeren gitt tilganger til nettverket og man kan logge på nettverket med AD Brukeren sin, som ikke bare er brukervennlig, men også svært effektivt for alle ansatte. AD Brukeren og Informasjonen som har blitt lagret om de blir slettet dagen etter utsjekk slik at vi ikke lagrer informasjonen lengre enn det vi trenger.

Videre så oppretter vi også AD Grupper og kontoer til alle ansatte som kan brukes på både gjestenettverket og ansattnettverket slik at de også kan få gjort jobben sin. Her er også passord hashet som gjestene sine for å forhindre at andre kan se slike private opplysninger & innloggingsinformasjon. Ansatsene kontra gjestene vil også ha en vanskeligere passord protokoll slik at ingen kan gjette passordene, samt at vi kan også innføre 2FA ved bruk av skjemautfylling og SMS-Kode. Slik forsikrer vi oss om at kun ansatte har tilgang.

Siden vi bruker Active Directory til å lagre brukerkontoer og grupper må vi også sikre serveren på en grei måte slik at ikke alle kan få tilgang. Dette gjør vi ved bruk av 2FA og strenge passord protokoller for å logge inn som flere apper og tjenester tillater oss å gjøre.

Nå videre til den siste logiske sikringen vi må benytte oss av, nemlig Brannmuren. Som tidligere nevnt hjelper denne oss med å filtrere ut uønsket trafikk og mulige skadelige aktører. På Brannmuren kommer vi til å legge inn IP-Blokkeringer på sider som er klassifiserte som Skadelige av ISPen, som nesten enhver har, og videre bør vi også legge til en type last balanserer som for eksempel blokkerer spesifikke IP-Adresser om mye data blir sendt på engang for å forhindre DDOS angrep

I tillegg til den logiske sikringen må vi også innføre fysisk sikring til nettverket. Dette involverer at vi må ha nøkkelkort for server og ruter & switch rom, samt at vi også må plassere enheter og kabler på smarte plasser. Her må kabler gå gjennom vegger og tak, samt at enheter som aksesspunkter må plasseres ut av rekkevidde til uvelkomne. Sammen med dette kan brannslukningsapparat og andre sikkerhetsmidler bli brukt for å forhindre andre skader.

# Del 2: Planlegging av App/Nettside

## Lag en skisse av appen og beskriv de viktigste funksjonene den vil ha

Da det kommer til å lage en App // Nettside har jeg valgt å ikke bare lage en liten skisse, men heller å kode en nettside med både frontend og backend funksjonalitet for å vise hva jeg tenker. Dette ble gjort med HTML, CSS, Javascript og Node.JS.

Det å lage en nettside/app til Skyggefjell Skibakkene var ikke ekstremt vanskelig og de viktigste funksjonene som befinner seg på nettsiden er allerede beskrevet i oppgaven. Hovedsakelig så er de 3 viktigste funksjonene på nettsiden Hotell/Rom Booking, Digitalt Skikort og Statistikk over skiturer.

Først for å forklare/beskrive Booking funksjonaliteten. Hvordan bookingen på siden vil fungere er veldig enkelt. Ved bruk av Firestore-Database kan vi enkelt definere/lage dokumenter om hvert hotellrom vi har og dens kostnad og informasjon. Denne informasjonen kan vi bruke til å dynamisk lage innhold på nettsiden vår og åpne rommene for både bestilling, men også «utstilling» og reklame.

Når man trykker på et rom kommer opp et popup på siden hvor man kan gå videre til bestilling / handlekurv, hvor man kan bestille rommet og legge igjen informasjon som E-Post, Telefon, Navn etc. slik at man kan bli kontaktet etterpå. Denne informasjonen vil også bli brukt til å lage en bruker for dem på nettsiden, slik at man faktisk kan bruke den kontoinformasjonen til å videre lage AD-Brukere og generelt gi ut digitale skikort i ettertid.

Her er det viktig at man spør om samtykke og informerer de klart og tydelig om hva som blir lagret, brukere blir opprettet og mer. Etterpå vil man ha tilgang til all booking informasjon, skiinformasjon og support funksjonalitet via «Min Side».

«Min Side» er brukernes personlige side hvor man kan se på ting som brukerinformasjon/innstillinger, Support og meldinger fra resorten ut til kundene, samt andre ting som skikort og statistikk over skiturene. Digitalt Skikort er den andre viktigste funksjonen på nettsiden og vil bli brukt til å få nett tilgang, få seg gjennom skiheiser etc. Her kan man benytte seg av QR-Koder om man ikke velger å bruke det fysiske til å scanne. Når man har sjekket inn blir skikortet aktivert digitalt, samtidig som at man mottar et fysisk kort, noe som gir de tilganger til ulike ting som tidligere nevnt. Ideen rundt digitalt skikort er at man kan logge inn med nettside brukeren på nettverket istedenfor å få et eget brukernavn og passord der også.

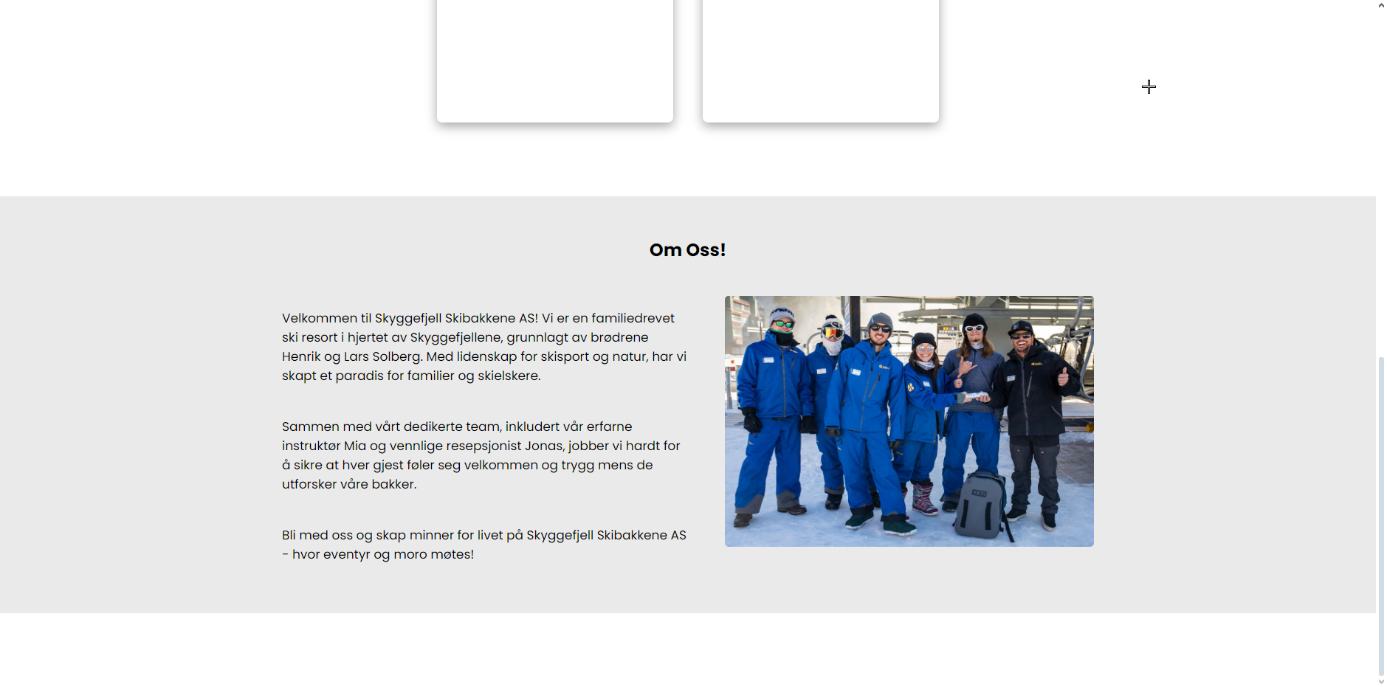
Sist, men ikke minst, «Statistikk» siden. Denne siden viser frem Skitur statistikken til besøkende som blant annet hvor mange meter de har kjørt oppe i bakkene, antall bakker kjørt ned og sist gang de var ute i bakken. Mer informasjon kan bli lagt til, men enn så lenge var dette det jeg fokuserte på og var fornøyd med. Nedenfor kan du se bilder av nettsiden og se hva jeg har laget 😊 Håper det er bra nokk!

Et bilde som inneholder tekst, bakke, skisport, skjermbilde

Automatisk generert beskrivelse

Et bilde som inneholder tekst, skjermbilde, design

Automatisk generert beskrivelse



Et bilde som inneholder tekst, skjermbilde, programvare, Font

Automatisk generert beskrivelse

Et bilde som inneholder tekst, skjermbilde, Font

Automatisk generert beskrivelse

## Beskriv database-designet og infoen den vil lagre og hvordan den er strukturert.

Når det kommer til Database har jeg valgt å bruke en Firestore-Database laget av google og drevet gjennom skyen til bruk i mitt prosjekt, men det skal sies at dette er kun brukt for å vise frem produktet enklere i casen, mens på ekte ville jeg ha brukt en lokal hostet database i stedet slik at den ikke er tilgjengelig for andre over offentlig nettverk. Databasen i den ekte løsningen vil være MongoDB, grunnen til dette ligger mest i at MongoDB er veldig lik Firebase og måten den fungerer på, dermed er det mye som ligner.

Både MongoDB og Firebase er begge såkalte NoSQL-Databaser, noe som er annerledes fra den tradisjonelle SQL Database som mange selskap og eldre produkter benytter seg av. Forskjellen mellom disse 2 databasene er at i NoSQL, lagrer vi dataen som såkalte «Dokumenter» med felt inne i seg, istedenfor at vi lagrer dataen i rader og kolonner som i SQL.

Grunnen til at jeg velger en slik løsning, er rett og slett fordi ved bruk av NoSQL trenger man ikke å vite like mye om SQL Queries som i den andre løsningen, samt at reglene rundt lagring av data i databasen er veldig åpne og man må ikke følge en satt «struktur» som man må i SQL.

For eksempel i SQL må alt data i en kolonne være samme datatype og som regel referere til en lik type verdi, mens i NoSQL kan 1 dokument i en kolleksjon ha feltet «Frokost: True/False», mens de andre trenger ikke å ha dette feltet i motsetning til SQL hvor man må ha det. Dette gjør arbeidet enklere og databasen litt mer brukervennlig, og ikke minst enklere å ha oversikt over. NoSQL er fremtidens database og derfor er det viktig å benytte oss av den nye standarden i Skyggefjells produkter også.

Nå som du/dere vet hvordan database jeg benytter meg av og baktanken bak valget kan vi gå videre til hva jeg faktisk skal lagre av data. Det som er viktig å tenke på når man skal lagre data er hovedsakelig hvordan den skal sikres, samt å ha et grunnlag for å lagre den informasjonen. Har man ikke et grunnlag for innsamlingen og kan heller ikke sikre dataen man lagrer er det ikke vanskelig å miste kontrollen. Derfor har jeg planlagt hva jeg skal lagre og hvorfor. Nedenfor er en liten liste på hva jeg skal lagre og hva skal de bli brukt til

* Brukerinformasjon
  + Navn, Epost, Telefonnummer og et eget konstruert passord vil bli lagret
* Kommer til å bli lagret sikkert i databasen. Her vil sikkerhet være på plass som MFA og ting som passord og eposter vil være hashet // umulig å lese av. Her kan BCrypt for eksempel bli brukt.
  + Ordreinformasjon // Historikk
    - Alle ordre som knyttes opp imot en aktiv konto kommer til å bli lagret i databasen slik at man kan se tilbake på det frem til man velger å avslutte kundeforholdet. Her vil Produktnavn/Rom, Pris, Innsjekk og Utsjekk,

samt hva tilbudet inneholdte bli lagret slik at man kan alltid se tilbake på hva man har betalt for tidligere, eller fremtidige betalinger. Dette vil kun kundene ha tilgang til.

* + Statistikk over Ski & Heisturer
    - Siden Skyggefjell Skibakker AS ønsket å benytte seg av kunde data til å lage en statistikk side/funksjon på appen må vi selvsagt også lagre denne informasjonen i vår database.
    - Her kommer vi til å lage 1 dokument for hver heistur som samler informasjon om dato & tid, antall meter tur og HeisID som kan spores mot enkelte bakker.
    - Denne informasjonen/statistikken vil bli plusset sammen i felter som «Antall Skiturer», «Antall meter dratt», «Sist Skitur» etc. Og vil bare være tilgjengelig på kundenes inviduelle side for statistikk. Hver uke/andre uke vil denne dataen bli slettet siden det er ikke grunnlag til å oppbevare slik personlig data i en lengre tid. Her må vi bevare personvern. Ingen andre vil ha tilgang på denne dataen.
  + Hotellrom til leie
    - Databasen kommer også til å selvsagt lagre all data om hotellrom på resorten, hvor de tilgjengelige rommene vil være synlig på nettsiden for booking. Her vil blant annet romnummer, type rom (single, dobble etc.), ulike pakketilbud og rombeskrivelse bli lagret og dermed brukt på nettsiden til å lage dynamisk innhold når et rom et tilgjengelig.

Et bilde som inneholder tekst, skjermbilde, Font

Automatisk generert beskrivelseEt bilde som inneholder tekst, skjermbilde, Font, programvare

Automatisk generert beskrivelse

Nå til slutt tenker jeg å oppsummere database designet mitt med å vise bilder av strukturen til databasen og vise det via tekst også. Slik er databasen min organisert/strukturert:

Skyggefjell Database (Hoved)

|\_\_\_\_ Hotellrom (Collection)

|\_\_\_\_\_\_ Rom Dokumenter (Dokumenter)

|\_\_\_\_\_\_\_\_ Rom Navn, Beskrivelse, Bildeadresse, Pris (Felt)

|\_\_\_\_\_\_\_ Tilbud (Sub-Collection)

|\_\_\_\_\_\_ Tilbud Dokumenter (Bare Rom, All Inclusive etc.)

|\_\_\_\_\_ Pris, Frokost (Boolean), Utstyr (Boolean) etc.

|\_\_\_\_ Registrerte-Brukere (Collection)

|\_\_\_\_\_ Bruker Dokumenter (Dokumenter)

|\_\_\_\_\_\_ Navn (Hash), Mail (Hash), Passord (Hash), TLF (Hash), Skikort etc.

|\_\_\_\_ Ordrehistorikk (Sub-Collection)

|\_\_\_\_\_ Ordre Dokumenter

|\_\_\_\_\_ Pris, Rom, Tilbud, Innsjekk/Utsjekk

|\_\_\_\_\_ Ski-Statistikk (Sub-Colletion)

|\_\_\_\_ Statistikk Dokumenter

|\_\_\_\_\_ Antall Heisturer, Siste Tur, Total lengde

|\_\_\_\_\_ Heisturer/Skiturer (Sub-Collection)

|\_\_\_\_ Lengde, Timestamp/Dato&Tid, HeisID

Databasen er organisert i egne kategorier relevant til dataen som blir lagret, slik at ting er hele tiden enkelt å sjekke på/holde oversikt over. **All Persondata i databasen skal bli sensurert / Hashet for å forhindre både uautoriserte brukere og ansatte fra å se alt i plain tekst.** Bare datamaskinen som faktisk har tilgang til å dekryptere dette, noe som ikke bare sikrer oss mot datatap og angrep, men også kundenes informasjon fra å bli tatt. Selv så mener jeg at den er godt planlagt og veldig godt organisert. (Se bilder nedenfor)

Et bilde som inneholder tekst, skjermbilde, Font, nummer

Automatisk generert beskrivelse

Et bilde som inneholder tekst, Font, nummer, programvare

Automatisk generert beskrivelse

Et bilde som inneholder tekst, skjermbilde, Font, nummer

Automatisk generert beskrivelse

Et bilde som inneholder tekst, skjermbilde, Font, nummer

Automatisk generert beskrivelse

# Del 3: Drøfting rundt datainnsamling og Personvern

## Hvilke fordeler og ulemper finnes innen innsamling av heistur data.

Når vi skal ta innsamling av personlig data som hvilke skiheiser man bruker og når, hvor mange meter man har dratt totalt etc. Mottar vi noen fordeler, men vi får også noen ulemper med på laget. Det å samle inn slik data kan lett misbrukes til feil hensikt, derfor er det viktig at man innfører tiltak rundt datainnsamlingen og oppbevaringen av data slik at den blir brukt til riktig formål og ikke annet.

### Fordeler

Ved å innsamle data om gjestenes heisturer kan vi for eksempel bruke dataen til å kartlegge hvilke bakker som er mest populære, og eventuelt hvilke som ikke er det, noe som kan bidra til at vi enklere kan forbedre og ha en oversikt over upopulære bakker / løyper. Dette kan jo hjelpe på både et opplevelses aspekt for gjestene, samt et inntektsaspekt for bedriften.

I tillegg til forbedringer og populære bakker kan man også bruke informasjonen til å **kartlegge hvilke bakker og heiser som kanskje må driftes/vedlikeholdes** mer oftere. Er det slik at en, eller flere, spesifikke bakker blir brukt absolutt mest, kan disse delene av resorten slites ekstra fort, noe som betyr at vi kanskje bør se på vedlikehold og ta en sjekk av utstyret oftere enn tidligere. Med andre ord kan denne statistikken hjelpe oss med å identifisere plasser som vi må ta kanskje litt ekstra vare på i tiden fremover.

Man kan også bruke tallene for blant annet reklamering og markedsføring/målsetting. Det å kunne kunngjøre at i desember hadde vi totalt 5000 Skiturer på sosiale medier og nettside kan bli brukt som en type **markedsføring**. Samtidig som at man kan også bruke tallene til å oppsummere hvordan ytelsen er i skibakkene. Er det slik at tallene går ned kjapt kan man se nærmere på heiser og hvilke løyper som har problemer, og motsatt om tallene går opp vet man at det går veldig bra for tiden.

### Ulemper

Ved innføring av slik datainnsamling kommer også flere ulemper med på kjøpet. Blant annet så kan innsamling av slik informasjon tvinge selskapet til å følge enda tettere med på prosedyrer rundt **datainnsamling, oppbevaring og sletting** slik at man tid enhver tid følger **personvernloven** og **GDPR**.

Slik data er ikke nødvendigvis sensitivt alene, men koblet sammen med annen data kan dette hjelpe og identifisere både personer og deres lokasjoner, med andre ord meget sensitivt med tilføyelse av ekstra data. Dermed kan man si at en ulempe blir jo såklart at ressurser og tid må legges inn til å sikre gode forhold rundt oppbevaring og innsamling av data, noe som er kostbart.

En annen ting er jo at registrering av hvilke heiser man tar til enhver tid over nett er jo i prinsippet en «text-book» definisjon på en **lokasjonssporer**. Med andre ord kan man enklere se hvilke bakker en person befinner seg i og hvor man kanskje oftest oppholder seg, noe som ikke akkurat er veldig bra å dele ut til andre. Her er det dermed viktig at man sikrer dataen ekstremt godt slik at bare kunden selv har tilgang til dette og ikke noen andre, Ansatt eller ei.

## Hvordan vil vi sikre at gjestene er klar over innsamlingen og sikre deres personvern

Først for å sikre at gjestene er klare over datainnsamlingen er det 2 viktige tiltak vi kan innføre. Det er **samtykke** og **informasjonsutgivning** over **nett** og **muntlig.** Her kan vi for eksempel innføre at man må lese gjennom et skjema å gi samtykke før man bestiller & oppretter bruker via nett, og informere om det samme muntlig da de sjekker inn slik at de er klare over hvordan man kobler seg på nett og hvilken data som blir lagret og hvorfor. Dette forsikrer oss om at de er fullt klar over ting som blir lagret, hvorfor og gir de rom til å spørre mulige spørsmål, eller nekte.

En annen måte vi også kan sikre personvernet til alle besøkende er rett og slett ved god tilgangskontroll. For å sikre et godt personvern må vi limitere hvor mange som har tilgang på opplysningene, hvordan man får tilgang og hvor lett det er i prinsippet å angripe systemet.

Ved bruk av MFA på nett og server, AD og eventuelt nøkkelkort dør for Windows Serveren vår, vil ikke bare database innloggingen være nesten umulig å knekke, men det vil også være så å si umulig å få fysisk tilgang til noe utstyr uten å være ansatt. Derfor er tilgangskontroll også en viktig del av løsningen vår. All sensitiv data som passord, e-post etc, Vil også være kryptert via hashing så ingen ansatte uansett tilgang eller ei kan se eventuelle opplysninger. Bare Serveren vil kunne bruke disse til å gjøre jobben sin, ingen andre.

I tillegg til begge disse 2 tiltakene er det også viktig å passe på at man opprettholder alle Personvernsprinsipper og følger regelverket. Med andre ord må man ha en gjennomsiktig databehandling som informerer kunden om innsamlinger, man må minimere dataen man har når man ikke lenger har bruk for den, man kan kun samle inn det som oppfyller kravene i formålet til bedriften etc. Her er det viktig å tenke på hva man samler inn, hvor lenge man har det og eventuelt hva man skal bruke det til. Dette må man også såklart informere om til både kunden og ansatte. Med andre ord må de på Skyggefjellet planlegge systemet rundt dette godt.

Med alle disse tiltakene på plass og god oppfølgning av regelverk vil personvernet være sikret og brukerne vil være informert om hva innsamlingene går ut på, som besvarer oppgaven i den fulleste grad.

Takk for at du har lest gjennom mitt dokument 😊