Oppgave 1

Noen verdier:

Sikkerthet

Autensitet.

Tilgangskontroll.

Personvern er viktig for elevene, siden informansjon om deres addresse, mobilnummer, navn og fødselsdato blir lagret på skolens datasystemer.

Integritet er viktig for lærerne fordi læreren må kunne være sikker informasjonen ikke feilaktig endres.

For en elev kan tilgjengeligheten være en viktig verdi, for å kunne se sin fremgang underveis. Mens for enn lærer er integriteten viktigere fordi resultatene skal være avsluttende

Oppgave 2

KIT-målene

Vurder viktigheten og hva som kan utgjøre en trussel.

En trussel mot konfidensialitet

Integritet:

Tilgjengelighet: Tilgjengelighet betyr at informasjon er tilgjengelig nøyaktig når en bruker trenger den informasjonen. I dette scenarioet er det viktig for både elevene og lærerne å ha tilgang til innleveringer og tilbakemeldinger, men også nyheter om endringer i ukeplaner, eksamenstrekk osv. En trussel mot tilgjenelighet kan være DoS (Denial of sevice) angrep, der enten en sentral enhet eller et desentralisert nettverk tetter skolenettverket med nettverksetterspørsler for å hindre legitim bruk av skolens datasystemer.

Konfidensialitet

Integritet

Tilgjengelighet

Oppgave 3

sikkerhetstiltak:

Sikkerhetstiltak som kan bidra til konfidensialitet er for eksempel two-factor authetication, autentisering med flere lag for å øke sikkerhet

1. Two factor authentication, kryptering
2. Kryptering, info puttet på blockchain

Oppgave 4

Sporbarhet og autentisering.

De er begge like viktige.

I nesten hvilket som helst datasystem, i dette tilfellet en videregående skole, der det er brukere skal ha tilgang til data gjennom internettet er både sporbarhet og autentisering ekstremt viktige sikkerhetsmål. Sporbarhet og autentisering henger sammen med hverandre til en stor grad. Sporbarhet; å spore hendelsene på et gitt system og å kunne tilknytte de hendelsene til en identitet. Autensitering innbærer å vite om en gitt identitet er *autentisk*, at en person er den de påstår å være. For en elev på denne videregående skolen ville dette innebært en innlogging(brukerautentisering) som krever et brukernavn(identifikator) og passord(autentiseringsfaktor). For å oppnå sporbarhet må systemet ha oversikt på alle identiter og handlinger, dette krever at autentisering allerede er oppnåd. Så må handlingene loggføres slik at de kan i etterkant bli analysert. Uten at de fungerer sammen ville det ikke vært mulig å identifisere trussler før eller etter de allerede har skjedd.

Oppgave 5

Det trengs en liste av brukere, og hvilket nivå av tilgang de har over hvilken informasjon.

Deretter trengs et system som kan autentisere en bruker som den de er, som bank id, eller liknende.

Så må informasjon deles ut i henhold til tillatelsene.

Oppgave 6

Siden man ikke vet hva begrunnelsen kan inneholde, burde alle behandles som om de inneholder besyttede personoplysninger. Systemet må derfor forsikre at informasjonen er trygt lagret (kryptert) og har streng kontroll over tilgang.

Man kunne bedt elev/forelder notere hvilket nivå personoplysninger det er snakk om, men dette fører til mer arbeid, stress for bruker og potensielle sikkerhetshull.

Oppgave 7

Det er viktig å kryptere trådløs nettverkdata (wifi/WLAN) fordi ukryptert data, selv om det blir filtrert ut av mange nettverkskort, er fortsatt åpen for de med riktig utstyr(kort med promiscuous mode). En trusselaktør kan enkelt bruke en laptop for å se på nettverkstrafikken din på et ukryptert trådløst nettverk. Dette er et relativt åpenbart sikkerhetsproblem. I forhold til å la elever og lærere dele trådløst nettverk er det tenkelig at en elev kan se på nettverkstrafikken lese andre elevers innleveringer på en prøve ved å sniffe packets.

Oppgave 8

Jeg hadde laget en klassisk phishing scam, altså en login nettside som er helt lik skolens login side(feks som feide) som lagrer brukernavn og passord. Jeg sender linken til læreren i det faget jeg har lyst til å endre karakter i (eller alternativt en sysadmin om det ikke fungerer). Hvis det fungerte er det bare å logge inn med lærerens brukernavn og passord for å utnytte tilgangen til å endre informasjon i systemet.