# Sjekkliste – Din digitale beredskapsplan Aktuelt Sikkerhet

**Har din virksomhet en digital beredskapsplan?**

I den digitale hverdagen vi lever i, er det viktig for enhver virksomhet å ha en digital beredskapsplan. Hva kan du gjøre for å unngå å bli offer for datakriminalitet, og hvordan kan du forberede virksomheten best mulig.

NSM har utarbeidet en ***sjekkliste*** over prioriterte tiltak virksomheter bør følge, særlig i en skjerpet sikkerhetssituasjon.

Virksomheter i dag bør på forhånd ha etablerte og gjennomførbare beredskapsplaner. I tillegg må de ansatte ha gjennomgått opplæring for å unngå menneskelige feil. Med et økende risikonivå verden over, er det desto viktigere å ha dette på plass. Det kan være krevende å gjennomføre raske endringer. Vi har derfor samlet sammen en sjekkliste, basert på det NSM anbefaler at dagens virksomheter iverksetter som en del av sin jobb med datasikkerhet.

**Har du kartlagt alle systemer virksomheten din bruker?**

____ Har du en oppdatert oversikt over systemer og programvare som kjører på nettverket til virksomheten?

____ Er alle maskiner oppdaterte?

____ Har du et vedlikeholds- og nettverkskart, samt oversikt over tilknytninger mot andre virksomheter?

## Dersom virksomheten din blir rammet av en hendelse, er dette helt nødvendig å ha på plass.

# Sjekkliste – Din digitale beredskapsplan
# Aktuelt Sikkerhet

**Har du sikkerhetskopier?**

____ Har du oppdaterte sikkerhetskopier av datasystemene som brukes i virksomheten?

____ Er disse lagret i et isolert system som har ekstra beskyttelse mot tilsiktet og utilsiktet sletting, manipulering og uthenting?

**Du bør verifisere jevnlig at det lar seg gjøre å gjenopprette både systemer og andre datasett fra disse sikkerhetskopiene.**

**Har du kontroll på sårbarhetsflaten til virksomheten?**

____ Har du kontroll på tjenester som kan være eksponert via internett?

____ Har virksomheten utstyr eller løsninger som bør fases ut?
Dette kan for eksempel være løsninger som mangler muligheten for to-faktorautentisering.

____ Har virksomheten flyttet tjenester og løsninger til skyen?

____ Har virksomheten kontroll på alt utstyr de ansatte bruker?
Både på kontoret og på hjemmekontoret?

**Digitalt beredskap handler om å fjerne gamle løsninger, disse har lett for å henge igjen, og bør derfor oppdateres for å øke sikkerheten.**

# Sjekkliste – Din digitale beredskapsplan
# Aktuelt Sikkerhet

**Identiteter og tilganger**

____ Har virksomheten en rutine for gjennomgang av brukere og tilganger?

____ Husk å fjerne brukere som ikke lenger skal ha tilgang, og sikre samtidig at brukerne ikke har tilgang til flere tjenester enn nødvendig.

____ Har alle brukere unike og sterke passord? Huks at to-faktorautentisering må på for alle tilganger.

____ Har virksomheten kontroll på hvem som trenger tilgang når og fra hvor?

## Husk å sørge for at alle innlogginger på web gjøres over HTTPS. Dette gjelder alle tjenester.

**Sikkerhetsovervåkning**

____ Har virksomheten en løsning for monitorering av systemer og nettverk?

## Dette kan for eksempel være loggføring på flere systemer. Det er helt avgjørende å kunne undersøke en hendelse dersom den inntreffer.

**Årvåkenhet blant ansatte**

____ Har virksomheten gjennomført tiltak som er rettet mot medarbeidernes sikkerhetskultur- og forståelse?

**Husk at skjerpede sikkerhetstiltak mot blant annet nettfiske og sosial manipulering kan bidra til økt årvåkenhet blant de ansatte. Spesielt gjelder dette for e-post, videomøter, digitale samarbeidsplattformer og sosiale medier. De ansatte bør få føringer til hvordan man kan sette sterke passord og aktivere to-faktorautentisering.**

# Sjekkliste – Din digitale beredskapsplan
# Aktuelt Sikkerhet

**Håndtering av hendelser**

____ Har virksomheten utarbeidet en beredskapsplan? Er denne oppdatert og gjennomprøvd?

____ Har virksomheten oppdaterte lister over kontaktpunkter blant relevante ansatte og tjenestetilbydere innen hendelseshåndtering?

**Det å ha fokus på et godt planverk gjør at virksomheten vil være i bedre stand til å håndtere uforutsette hendelser.**

**Verdikjeder og tjenesteutsetting**

____ Har virksomheten kontroll på de ulike leverandørkjedene?

____ Har virksomheten en oversikt over leverandører av systemer og tjenester?

**Leverandørkjeder kan representere sårbarhetsflater for digitale angrep. Det er derfor veldig viktig at disse er med i beredskapsplanen.**

**Forsterk beskyttelsen av skytjenester**

____ Har virksomheten opprettet tilgangskontroll og sikkerhetsbarrierer når det kommer til skytjenester som er utenfor virksomhetens infrastruktur?