|  |
| --- |
| **Retningslinjer for sikkerhetstiltak ved Ditt firmanavn AS**  |
| **Utarbeidet av:**  | **Godkjent av:** | **Dato:** 00.00.00 |
| **Dokument ID:** | **Neste revisjon:** | **Versjon:**1 |

**Begrensninger for ansatte i organisasjonen:**

* Aldri lagre passord på nettlesere. Alle passord må huskes og ingen skal lagres automatisk.
* Aldri ta med personopplysninger om kunder, ansatte, kollegaer eller andre hjem fra jobb, dersom dette kan unngås.
* Slette personopplysninger man ikke absolutt må oppbevare fra innbokser i kommunikasjonskanaler som E-post, Slack, Facebook@Work osv, hver dag før man drar fra jobb.
* Samle alle personsensitive dokumenter man må oppbevare på jobb pc/privat pc i en egen mappe på skrivebordet der man legger på en ekstra passordbeskyttelse.
* Aldri bruke private mobiltelefoner til å lagre personinformasjon på kunder.
* Alle dataenheter som brukes i jobbsammenheng må ha passordbeskyttelse på selve enheten.
* Alle ansatte må få beskjed om at datamateriale, enheter og dokumentasjon som kan inneholde person informasjon tilhører bedriften og må leveres tilbake eller slettes ved opphør av arbeidsforholdet.

I tillegg må det opplyses om at de kan bli holdt juridisk ansvarlige jamfør taushetsplikten sin dersom brudd på personvernloven oppstår som resultat av dårlige rutiner hos den ansatte. Dette bør inn i arbeidsavtalen som en egen klausul.

**Andre sikkerhetstiltak og rutiner:**

* Passordbeskyttelse for å hente ut noe fra printer
* Lås på dørene til kontorene
* Kortleser inn til lokalet hele døgnet, der kun de med riktig autorisasjon har adgang
* Passordbeskyttelse på alle enheter som behandler informasjon i bedriften.
* Tilstrekkelig fysisk sikring av backup-systemer
* Jevnlige internkontroller og gjennomganger av alle rutiner som er nevnt i dette dokumentet.

**Sikkerhetsrutiner for rekruttering og oppsigelser.**

* Cv-er oppbevares i egen passordsikret mappe på skrivebordet. Skal kun deles med personer som skal være med i vurderingsprosessen.
* Cv må slettes senest 6 måneder etter at prosessen er avsluttet dersom man ikke har valgt å gå videre. Kan ikke lengre oppbevares i tilfelle senere behov.
* Ved avslutning av ansattforholdet må Cv-er slettes innen den samme 6 måneders perioden Datatilsynet har satt som veiledende.

Dersom man ønsker å ta vare på denne lengre enn anbefalt må man behovet gjennom kartleggingens verktøyene og dokumentere hvorfor man ønsker å oppbevare det, hjemmel for oppbevaringen og hvor lenge. Samtidig må vedkommende gjøres oppmerksom på det og gi sitt samtykke.

* Notater som gjøres i forbindelse med vurderingene av en ansettelse, sammen med tester og annet materiale vedkommende kan identifiseres med, må behandles som informasjon på samme måte som CV-en. I tillegg må det som noteres skrives på en slik måte at arbeidssøkeren/-takeren kan få se det som er skrevet dersom denne ønsker det.
* Ved oppsigelser må ansatte slette sine egne dokumenter på arbeidsenheter eller få beskjed om at dette slettes (formateres) uten backup automatisk etter at bedriften ikke er juridisk bundet av en arbeidsavtale eller andre prosesser som lovlig hindrer bedriften fra å slette den ansattes lagrede data. Samtidig må det inn i arbeidskontraktene at arbeidstaker plikter å oppgi og videresende all dokumentasjon som tilhører bedriften til IT ansvarlig før denne fratrer sin stilling. Dette for å sikre at bedriftens produserte verdier ikke blir borte samtidig.
* Tilganger, kodekort og eventuelle nøkler må fratas med en gang siste arbeidsdag er gjennomført slik at vedkommende ikke kan få adgang til datamateriale tilhørende bedriften. Adgang må eventuelt begrenses gjennom kort og kodesystemet dersom fysiske tilgangsmidler ikke blir levert. Her kan også sluttoppgjør og feriepenger med mer holdes tilbake inntil vedkommende har levert disse med hjemmel i risikoen dette medfører.