# Sikkerhetsinstruks – bruker

|  |
| --- |
| Punktene om privat bruk og arbeidsgivers innsyn i e-post og filer bør vurderes konkret for virksomheten. Når innsyn er tillatt og hvordan arbeidsgiver i så fall skal gå frem, er regulert i en egen forskrift (les mer <https://www.datatilsynet.no/personvern-pa-ulike-omrader/personvern-pa-arbeidsplassen/innsyn-epost-filer/>). Instruksen må gjøres forutsigbar og konkret for brukeren. Instruksen bør gjennomgås med tillitsvalgte før den tas i bruk i virksomheten.  |

Her er de viktigste reglene om IKT-sikkerhet som vi skal forholde oss til i det daglige. Mer detaljerte regler finner du i andre rutiner i internkontrollen.

*<Nedenfor beskrives klassifisering av informasjon direkte i instruksen. Det er også mulig å ta det ut av dette dokumentet og i stedet opprette et eget dokument kalt «Informasjonshåndtering».>*

## Klassifisering av informasjon

Vi bruker her tre beskyttelsesnivå for informasjonen – åpen, intern og kritisk med hensyn til konfidensialitet.

* **Åpen informasjon** er informasjon uten beskyttelsesbehov, slik som publikasjoner, dokumenter som er vurdert som offentlige (forhåndsvurdert av arkiv, gitt innsyn i eller publisert) og presentasjoner vi har holdt.
* **Kritisk informasjon** er alle dokument med et høyt beskyttelsesnivå mht. konfidensialitet. Dette inkluderer:
	+ Sensitive personopplysninger (med unntak for det lite beskyttelsesverdige)
	+ Opplysninger om personlige forhold hvor lekkasje kan få alvorlige konsekvenser for enkeltpersoner - som ved en arbeidslivskonflikt
	+ Opplysninger om forhold hvor lekkasje kan få alvorlige konsekvenser for eksterne virksomheter eller *<Virksomhet>* (og hvor forholdet ikke skal være offentlig kjent)
	+ Opplysninger av betydning for andre virksomheters informasjonssikkerhet
	+ Opplysninger av betydning for *<Virksomhet>s* informasjonssikkerhet
* **Intern** **informasjon** er all annen informasjon. Dette inkluderer:
	+ Alle dokumenter på filområder som ikke er vurdert mht. offentlighet
	+ Alle dokumenter som er vurdert som ikke-offentlige (men ikke kritiske)
	+ Alle dokument om interne forhold i *<Virksomhet>*
	+ E-postkommunikasjon internt og eksternt
	+ Notater og skriblerier (inklusive post-IT, saksomslag etc.)

## E-post

Kritisk informasjon skal ikke sendes på e-post.

* Dersom det er mottatt e-post med kritisk informasjon skal e-posten legges inn i saksbehandlingssystemet. Opprinnelig melding (og eventuelle kopier av denne) skal slettes.
* Sjekk at mottakeradressene er korrekte før e-poster sendes.
* Vedlegg og lenker skal ikke åpnes dersom du ikke stoler på innholdet. Husk at e-poster konstruert for phishing kan se ut til å komme fra en kollega.
* Brukeren har selv ansvar for å opprette egen mappe som er tydelig merket «privat», for lagring av privat e-post.

## Internett

*<Virksomhet>* identifiseres ved all bruk av internett fra våre systemer. Ta hensyn til dette.

Internett skal brukes for virksomhetsrelaterte formål, slik som i forbindelse med e-post og surfing. Det er tillatt med noe privat bruk. Eksempler på akseptabel og uakseptabel bruk:

**Akseptabel bruk**

* Nettaviser, nettbank, hjemmesider og informasjonssider
* E-post (også nettbasert privat e-post)
* Sosiale nettsteder som Facebook, Twitter, YouTube og lignende

**Uakseptabel bruk**

* Løsninger som unødvendig belaster nettverket og hvor det ikke er tjenstlig behov
* Installasjon av programvare uten avklaring med IT-ansvarlig
* Oppslag på nettsteder som kan skade *<Virksomhet>s* omdømme eller sikkerhet. Eksempler: pornografi, gambling, og nettsteder som sprer skadevare. Ved tjenstlig behov for slike oppslag skal sikkerhetsansvarlig kontaktes på forhånd
* Brudd på norsk lov og åndsverkregler
* Brudd på *<Virksomhet>s* etiske regler

## Sikkerhet på eget kontor

Dokumenter som inneholder kritisk informasjon skal ikke ligge åpent tilgjengelig for uvedkommende.

Lagringsmedium (for eksempel minnepinner) med intern informasjon skal ikke ligge åpent tilgjengelig.

Når man forlater kontoret i løpet av arbeidsdagen skal maskinen låses umiddelbart (Windowstasten + L).

Ditt personlige passord til *<Virksomhet>* skal ikke skrives ned eller oppgis til andre. Bruk et eget passord til din brukerkonto i *<Virksomhet>*, og ikke det samme passordet som du bruker på tjenester utenfor *<Virksomhet>* (for eksempel på privat e-post eller sosiale medier). Passordråd finnes her: <https://nettvett.no/passord/>

Passord skal skiftes straks bruker er kjent med, eller har mistanke om at andre har skaffet seg kunnskap om passordet.

Kontordøren skal låses når kontoret ikke benyttes (ferie, kurs, når man går for dagen).

## Lagring og sikkerhetskopiering

Saksbehandling skal foregå i saksbehandlingssystemet. Her er det varig sikring av integritet og tilgjengelighet (sikkerhetskopiering).

Andre dokumenter skal som hovedregel lagres på hjemmeområder og fellesområder. Filer som er lagret der blir automatisk sikkerhetskopiert flere ganger daglig.

Brukeren har selv ansvar for å opprette egen mappe som er tydelig merket «privat», for lagring av personlige dokumenter.

## Utskrift, kopiering og makulering

*<Beskriv rutiner for utskrift, for eksempel om virksomheten benytter et felles utskriftssystem. Om systemet har en «follow me»-løsning, hvor brukere må identifisere seg med kort, nøkkelbrikke eller brukernavn/passord ved hver utskrift.>*

Dokumenter må ikke bli liggende på kopimaskin/skriver.

Dokumenter eller notater skal ikke kastes i vanlig søppelkasse. Bruk låst kontainer for sikkerhetsmakulering til alle andre dokumenter enn publikasjoner.

CD-er, minnepinner etc. skal leveres til sikkerhetsansvarlig. CD-er som sidestilles med publikasjoner kan kastes.

Rutiner ved besøk og servicepersonell
Alle besøkende skal hentes av den det er avtalt møte med.

Besøkende skal som en hovedregel følges. Tiltrodde besøkende som kan ferdes på egen hånd, skal utstyres med besøkskort som bæres synlig (som servicepersonell i enkelte tilfeller). Se egen rutine for dette.

Ved arrangement med mange besøkende skal arrangementsansvarlig følge egen rutine for sikker gjennomføring.

## Rutine for låsing og aktivering av alarm

*<Fyll ut hva som er rutiner for låsing og aktivering av alarm, samt sjekkliste for den siste som forlater arbeidsplassen ved endt arbeidsdag.>*

## Fjerntilgang

*<Beskriv om virksomheten har lagt til rette for at ansatte kan få tilgang til interne systemer og ressurser. Om det gjøres via en kryptert VPN-løsning, om løsningen benytter tofaktor-autentisering (den ansattes passord og engangskode), og om det kun kan benyttes fra <Virksomhet>s bærbare PC-er.>*

## Bruk av mobiltelefoner og nettbrett

*<Virksomhet>* gir de ansatte mulighet for tilgang til e-post og kalender på mobiltelefon og nettbrett. Dette gjelder også på enheter som eies av den ansatte*.*

*<Beskriv om det benyttes for eksempel et Mobile Device Management-system (MDM-system) for å sikre <Virksomhet> nødvendig konfigurasjonskontroll av enhetene.>*

Mobiltelefoner og nettbrett skal ikke på annen måte kobles til *<Virksomhet>s* informasjonssystem eller den ansattes arbeidsstasjon (for eksempel for synkronisering av e-post/kalender, oppdatering av programvare over internett, nedlasting av musikk). Ved eventuell lading av mobiltelefon via PC, skal den ansatte sperre for filoverføring, enten ved bruk av USB-strømpe eller ved å velge «kun lading» på mobiltelefonen.

Mister man mobiltelefonen sin eller på annen måte mistenker at andre har tilgang til informasjon på mobilen (som SMS-er), skal man straks si ifra til sikkerhetsansvarlig. Dette gjelder også hvis man mistenker at brukernavn og passord er kommet på avveier, eller at man bare ønsker å være på den sikre siden.

## Kommunikasjon og deling av filer eksternt

**Akseptabel bruk**

* *<Virksomhet>s* krypterte VPN-løsning
* Kryptert minnepenn benyttes for all intern informasjon
* Ukryptert minnepenn kan benyttes til åpen informasjon
* Bruk av mobiltelefon som trådløs sone.

**Uakseptabel bruk**

* Sending eller lagring av *<Virksomhet>s* informasjon på ikke-godkjente systemer (for eksempel privat e-post, skytjenester eller eksterne chatteløsninger)
* Lagring av kritisk informasjon på minnepenn, selv om den er kryptert

For særskilte behov, ta kontakt med sikkerhetsansvarlig.

## Taushetsplikt

Det er egne regler for taushetsplikt, og den ansatte signerer taushetsplikterklæringen ved oppstart av ansettelsesforholdet.

Husk at vi også skal ta hensyn til taushetsplikten internt, både ved bruk av fagsystem og i dialogen mellom kollegaer. Det skal ikke søkes tilgang til taushetsbelagt informasjon i våre systemer uten at det foreligger tjenstlig behov.

Vær varsom i dialogen med eksterne, inklusive familie og tidligere kollegaer.

## Avvik

Et avvik er en uheldig hendelse eller et regelbrudd, og er noe som skjer i alle virksomheter. Brudd på disse reglene, og internkontrollen forøvrig, skal rapporteres til sikkerhetsansvarlig som avvik. Meld straks fra til sikkerhetsansvarlig dersom du oppdager sikkerhetsbrudd eller hendelser som kan ha betydning for sikkerheten.

Mindre alvorlige avvik (for eksempel kollegaer som glemmer å låse datamaskinen) kan tas direkte med den det gjelder.

Det skal være en lav terskel for å rapportere avvik. Meld også fra om situasjoner hvor noe kunne gått galt, slik at vi kan forbedre oss.

Sikkerhetsinstruksen er lest og akseptert

Sted og dato: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Navn (blokkbokstaver): \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Signatur: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_