Informasjonshåndtering

NB! Innholdet i denne malen må tilpasses til egen virksomhet. Det kan medføre utfylling av ytterligere informasjon og/eller sletting av ikke relevant informasjon.

Det gjøres oppmerksom på at eksempelet kan være mer omfattende enn minimumskrav etter personopplysningsloven.

Innledning

Dette dokument er et vedlegg til Sikkerhetsinstruks bruker, ref. .

Klassifisering av informasjon

Informasjon som behandles i <virksomhet> har forskjellig beskyttelsesbehov og er delvis regulert av lovverk. For at brukere skal kunne vite hvordan man skal håndtere informasjonen, gis det i dette dokumentet definisjon av ulike typer informasjon, samt en tabell som viser hvordan den enkelte informasjon skal håndteres.

Følgende beskyttelsesgrader benyttes:

Klassifisering av informasjon	
Beskyttelses-grad	**Beskrivelse**
ÅPEN[1]	Åpen informasjon er informasjon som er åpent tilgjengelig for alle.
LAV (<Virksomhet> INTERNT)	Informasjon for internt bruk hvor kompromittering, tap eller utilgjengelighet kan føre til: o Uønsket offentliggjøring i media av informasjon som bare skal være tilgjengelig for ansatte o Mindre økonomiske tap o Mindre skade på <virksomhet>s renommé. o Eksempler på informasjon: Interne notater, rundskriv og presentasjoner
MIDDELS	Benyttes dersom det vil kunne *skade* offentlige interesser, en bedrift, institusjon eller enkeltperson at dokumentets innhold blir kjent for uvedkommende. Informasjon hvor kompromittering, tap eller utilgjengelighet kan føre til: o At informasjon om <virksomhet> som oppfattes som middels beskyttelsesverdig, kan bli lest/endret av uvedkommende. o Skade på <virksomhet>s renommé. o Risiko for økonomiske tap – under <> kr Eksempler på slik informasjon: o Personopplysninger o Strategier o Adgangskoder
HØY	Benyttes dersom det vil kunne forårsake *betydelig skade* for offentlige interesser, en bedrift, institusjon eller enkeltperson at informasjonen blir kjent for uvedkommende. Informasjon hvor kompromittering, tap eller utilgjengelighet kan føre til: o At informasjon om <virksomhet> som oppfattes som sensitiv, kan bli lest/endret av

[1] Dokumenter med åpen informasjon trenger ikke merkes med beskyttelsesgrad

	uvedkommende. o Alvorlig skade på <virksomhet>s renommé. o Risiko for økonomiske tap – over <> kr Eksempler på slik informasjon: o Sensitive personopplysninger o Sensitive opplysninger om virksomhetens strategi, planer og aktiviteter o Svært sensitiv informasjon om sikkerhetsrelaterte hendelser o Systempassord og andre passord
U.off	Unntatt offentlighet Brukes av offentlige etater. Man må henvise til hvilken paragraf dokumentet unntas etter.

Rutiner for informasjonshåndtering

	ÅPEN	INTERNT)LAV- (VIRKSOMH	Unntatt off.	MIDDELS	HØY
1 Merking					
Dokumenter / informasjon skal være merket med beskyttelsesgrad.		x	x	x	x
Dokumentet / informasjonen skal merkes med hvilken bestemmelse som gir hjemmel for å unnta dokumentet fra offentlighet.			x		
Angi eventuell tidsbegrensning for graderingen					
2 Kopiering					
Dokumenter skal bare kopieres til personer som har autorisasjon for graderingen.		x	x	x	x
3 Oppbevaring					
Ethvert tap eller kompromittering av beskyttelsesverdige dokumenter skal meldes til Sikkerhetsansvarlig og nærmeste linjeleder.		x	x	x	x
Lagres på sikkert område på filsystem hvor kun den/de som skal ha informasjonen har tilgang			x	x	x
Forhindre innsyn fra utenforstående		x	x	x	x
Skal være nedlåst når ikke under oppsyn			x	x	x
Utskrifter					
Utskrifter skal hentes umiddelbart fra skrivere slik at konfidensialitet (”Need to know”) i saksbehandlingen opprettholdes			x	x	x
På reise/Hjemme:					
Dokumenter/elektroniske medier skal oppbevares under oppsyn av den ansatte eller avlåst			x	x	x
Lagres kryptert på bærbar PC, eller annet portabelt utstyr			x	x	x
4 Forsendelse/elektronisk håndtering					
Fysiske dokumenter (papir) sendes i posten i lukket konvolutt	x	x	x	x	x
Skal ikke overføres som e-post på Internett					x
Sendes som kryptert fil / kryptert vedlegg til e-post på Internett Sørg for å få kvittering fra mottaker om at e-posten er mottatt.			x	x	
Kan sendes som normal (ukryptert) e-post	x	x			
Tillatt å sende på telefax	x	x			
Informasjonen skal ikke kommuniseres på steder hvor samtale kan overhøres av utenforstående.			x	x	x

	ÅPEN	INTERNT)LAV- (VIRKSOMH	Unntatt off.	MIDDELS	HØY
5 Journalføring					
Føres i journal unntatt offentlighet (ved mottak / forsendelse)			x	x	x
Føres i åpen journal (ved mottak / forsendelse)	x	x	x[2]	x[2]	
6 Makulering av dokumenter					
Papir legges i egne makuleringsdunker		x	x	x	x
Papir kastes i papiravfall / avfall	x				
7 Håndtering av datalagringsmedia					
Disker, utstyr som inneholder harddisker og annet lagringsmateriale (f.eks. minnebrikker, backuptape etc.), skal leveres til IKT-kontoret for forsvarlig destruksjon.	x	x	x	x	x
Lagringsmedia som CD, DVD og floppy-disker leveres til IKT-kontoret for destruksjon			x	x	x
Lagringsmedia som CD, DVD og floppy-disker klippes/brekkes i biter og kastes i avfall	x	x			
Reparasjon / Service*:*					
Datautstyr sendes IKT-kontoret	x	x	x	x	x

Referanser

[1] Personopplysningsloven m. forskrifter
http://www.lovdata.no/all/nl-20000414-031.html

[2] Sikkerhetsinstruks - brukere for <virksomhet>

[2] Hvis det føres offentlig journal, kan disse føres i åpen journal i stedet for journal unntatt offentlighet dersom journalføringen ikke røper fortrolige opplysninger. Nøytrale kjennetegn, utelatelser eller overstrykninger skal benyttes i kopi av journal som legges frem for publikum for å unngå at fortrolig informasjon røpes
[2]