

UiT

**NORGES
ARKTISKE
UNIVERSITET**

Informasjonssikkerhet

– med spesielt blikk på administrative funksjoner

Ingvild Stock-Jørgensen
Juridisk seniorrådgiver
UiT Norges arktiske universitet



Innledning

- Om meg
- Tema for dagen
 - Hva er informasjonssikkerhet og hvorfor er det viktig?
 - Hvorfor er det viktig?
 - Hva betyr det for administrativt ansatte og prosesser?

Hvorfor fokusere på informasjonssikkerheten?

- Ivareta institusjonens verdier
- Lovkrav m.m.

Eksempelvis:

- Personopplysningsloven og personvernforordningen (GDPR)
 - eForvaltningsforskriften § 15
 - Annen særlovgivning
-
- **God informasjonssikkerhet er en forutsetning for digitalisering**

Hva omfattes?

- **Kun personopplysninger?**

Nei, all informasjon som virksomheten forvalter

- **Kun den digitale behandlingen som er relevant?**

Nei, alle aspekter må behandles

Informasjonssikkerhet og personvern

- Er personvern og informasjonssikkerhet det samme?

Nei

- Er personvern mer enn informasjonssikkerhet?

Ja

- Er informasjonssikkerhet mer enn personvern?

Ja



UiT Norges arktiske universitet

Hva er informasjon

- Hva forbinder du umiddelbart med informasjon?
- Det at informasjon ikke er offentlig
– Uvedkommende skriftlige og elektroniske personopplysninger
- **Konfidensialitet**
– Kanskje det som er klassifisert
– Eksempel på klassifisering

Grønn	Gul	Rød	Svart
Åpen	Intern	Fortrolig	Strengt fortrolig

- Men dette er bare en av

Informasjons- sikkerhet

Så å

Hva skal ivaretas?

Informasjonens...

- **Konfidensialitet**
 - Ingen uvedkommende skal få tilgang
- **Integritet**
 - Ingen uautoriserte eller uaktsomme endringer
- **Tilgjengelighet**
 - Når du har behov for informasjonen skal den være tilgjengelig

Ivaretagelse av informasjonssikkerhet handler om å sikre disse tre* aspektene

Kan alt ivaretas samtidig?

- Som regel ikke
- Disse tre dimensjonene...
 - Konfidensialitet
 - Integritet
 - Tilgjengelighet

... er ikke alltid kompatible med hverandre

Roar Thon, NSM: «*Hva er det verste som kan skje? Det kan skje verre ting med journalen din enn at uvedkommende får innsyn i den*».

Så hva gjør man da?

- Noen spørsmål må stilles:
 - Hva medfører størst risiko?
 - Hva er viktigst å ivareta?
- At f.eks tilgjengelighet må få prioritet over konfidensialitet betyr *ikke* at man skal «se helt vekk» fra konfidensialiteten. På ingen måte.
- Hvordan finne ut hva man skal gjøre, hvordan prioritere, hvilke risikoer man kan og skal løpe?

Risikovurdering

Risikovurderinger

- Ingenting er 100 %. Uansett.
- Det vil alltid være en restrisiko, uansett hvilke og hvor mange tiltak man innfører
- Men hva er akseptabel risiko?
 - Kan være styrt av virksomhetens egne krav, lovkrav mv.
- Viktig å se gevinstene
- Svært viktig å starte tidlig nok med risikovurderingen

“If the highest aim of a captain were to preserve his ship, he would keep it in port forever”

- Thomas Aquinas

Hva er en risikovurdering?

Fordeling av de ulike risikoene, totalt: 33

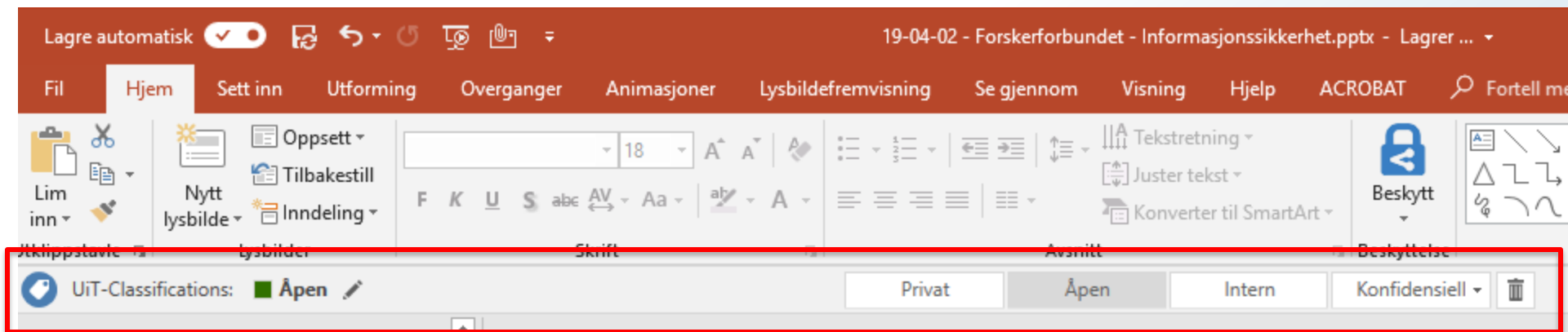
Konsekvens	4 Svært høy	T3, T10			
	3 Høy	P1, P2, P9, T4, T7, M2	T2, M4, M5	M6, M7, M8	
	2 Moderat	P3, P4, P11, P12, P14, T1	P5, P7, P8, T5, T6, M1	P6, P10	
	1 Lav	T8, T9, M3, M9		P13	
		1 Lav	2 Moderat	3 Høy	4 Svært høy
		Sannsynlighet			

Hva gjør man så?

- Tiltak
 - Redusere sannsynligheten og/eller konsekvensen
 - «Tekniske og **organisatoriske** tiltak»
- Vurdere nytteverdien av tiltakene
 - Kost/nytte
- Prioritere og beslutte hvilke som skal gjennomføres
- Vurdere hvilken risiko man står igjen med. Er denne akseptabel eller ikke?
 - Viktig at denne vurderingen tas på tilstrekkelig høyt nivå.

Hva betyr det for «den jevne ansatt»?

- Viktighet av at rutiner, brukerveiledninger faktisk følges
 - Tiltak kan ofte være rutiner,
 - eller en kombinasjon mellom tekniske tiltak og rutiner
- *Eksempel:*



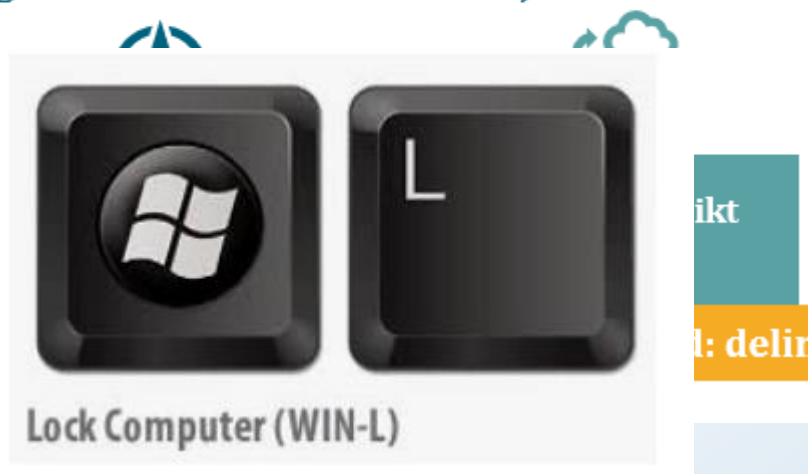
Sikkerhetskultur

- UiTs strategi for informasjonssikkerhet (2019-2021)
- Vaner

Eksempelvis:

2. MÅLBILDE

Figur 2 - Målbilde for informasjonssikkerhet i



Så åpen som mulig og så



Meld avvik!


- Avgjørende for å bli bedre
- Avviksmelding er **ikke**
 - Sladring, angiveri, flaut, kritikkverdig, unødvendig etc.
- Særdeles viktig at alle avvik meldes
 - Kan være både hendelser som har inntruffet, eller «nesten-ulykker».
 - brudd på rutiner vil være et avvik
 - Men det gikk jo bra, hvorfor skal jeg da melde fra?
 - Noen avvik må meldes til Datatilsynet og berørte personer – da løper tiden fort
- Oppfølging av risikovurdering

Så i sum?

- Informasjonssikkerhet må være en naturlig del av alle arbeidsprosesser
 - Tenk parallell til HMS
- Sikkerhet er mer enn å holde ting «hemmelig»
- Det omfatter all informasjon, ikke bare personopplysninger
... og alle typer behandling, ikke bare den digitale

Spørsmål?

Så åpen som mulig og så sikker som nødvendig

The bottom right corner of the slide features several decorative lines. A white line starts from the bottom right and extends towards the top right. A dark teal line starts from the bottom right and extends towards the top left. A light blue line starts from the bottom right and extends towards the top left, crossing the other lines.