



IKT-sikkerhet for arkivarer

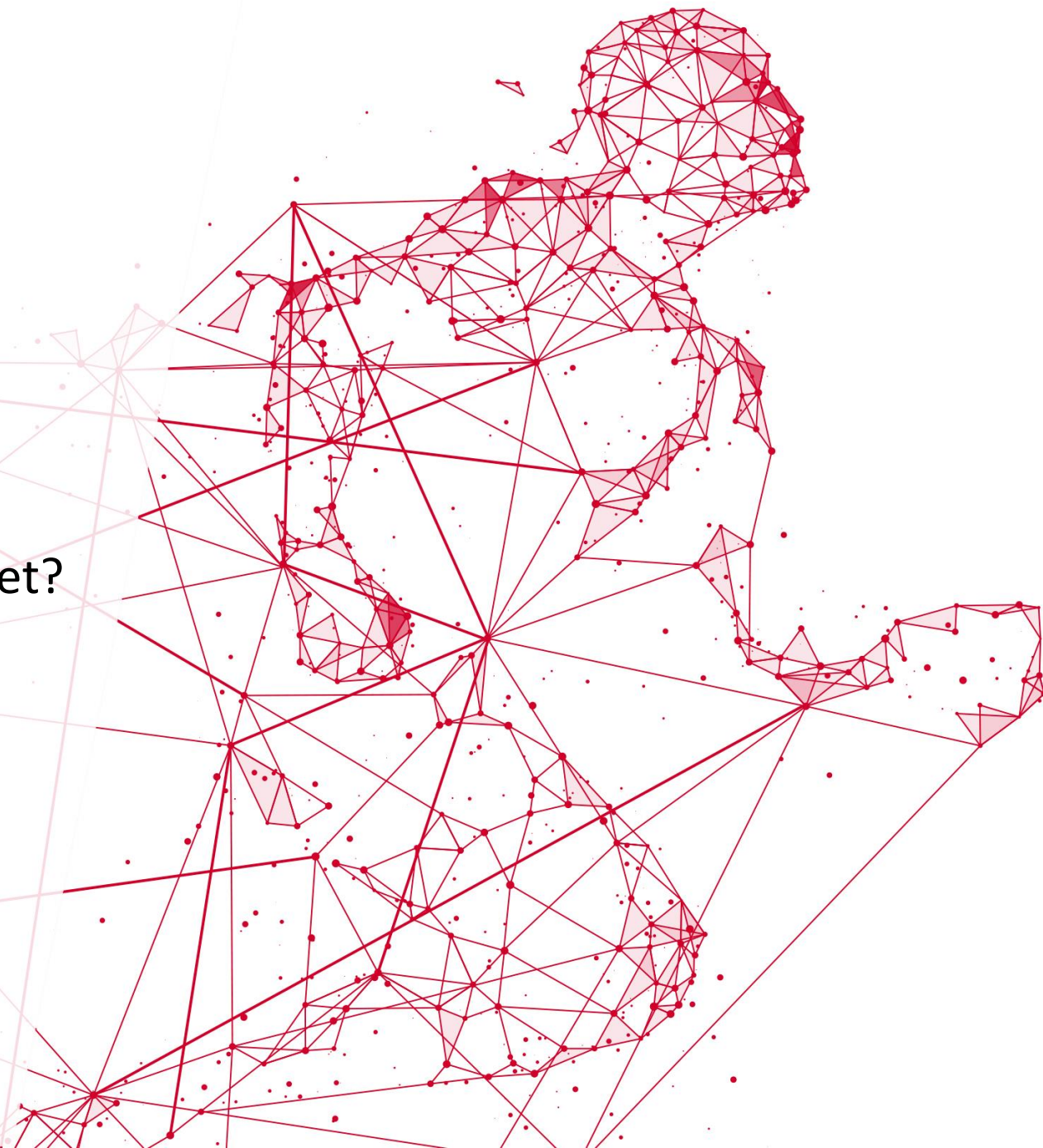
Kristine Synnøve Brorson

06.03.2018



Agenda

- Hva har IKT-sikkerhet å gjøre med dokumentasjonsforvaltning?
- Hvorfor holder det ikke at IKT-avdelingen sysler med IKT-sikkerhet?
- Hvordan kan IKT-sikkerhet bli inkludert i arkivplanen?

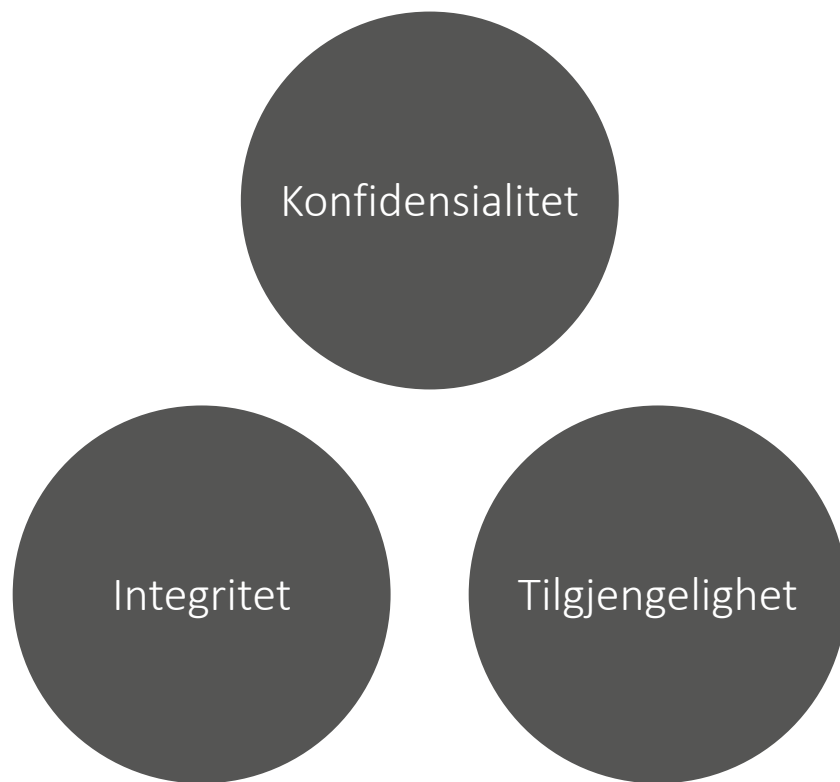




Hva har IKT-sikkerhet å gjøre
med
dokumentasjonsforvaltning?



Informasjonssikkerhet



KONFIDENSIALITET

Konfidensialitet er å sikre at ikke andre enn de som skal ha tilgang til informasjonen har tilgang.

INTEGRITET

Integritet er å sikre informasjonskvalitet. Det å sikre at dataene ikke er feil eller foreldet.

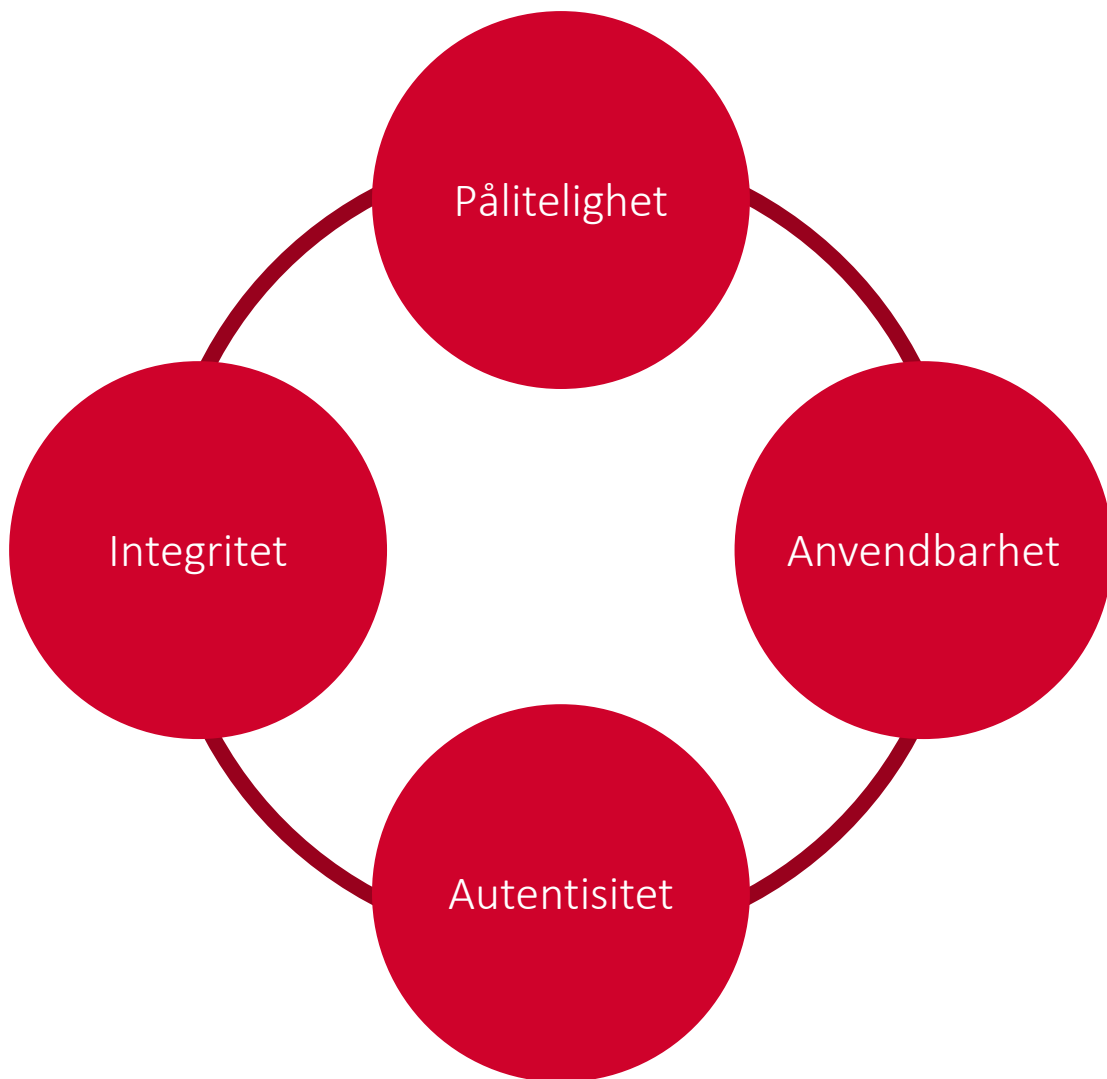
TILGJENGELIGHET

Tilgjengelighet er å sikre at de som skal ha tilgang på informasjonen har tilgang.

Definisjon fra ISO 27 000



Dokumentasjonsforvaltning



PÅLITELIGHET

Pålitelig dokumentasjon har et innhold som en kan stole på er en fullstendig og nøyaktig gjengivelse av transaksjonene, aktivitetene og faktaene som skal dokumenteres, og skal kunne danne grunnlag for etterfølgende transaksjoner og aktiviteter. transaksjonen.

ANVENDBARHET

Anvendelig dokumentasjon kan gjenfinnes, hentes frem, presenteres og tolkes.

INTEGRITET

At dokumentasjon har integritet, innebærer at den er fullstendig og uendret

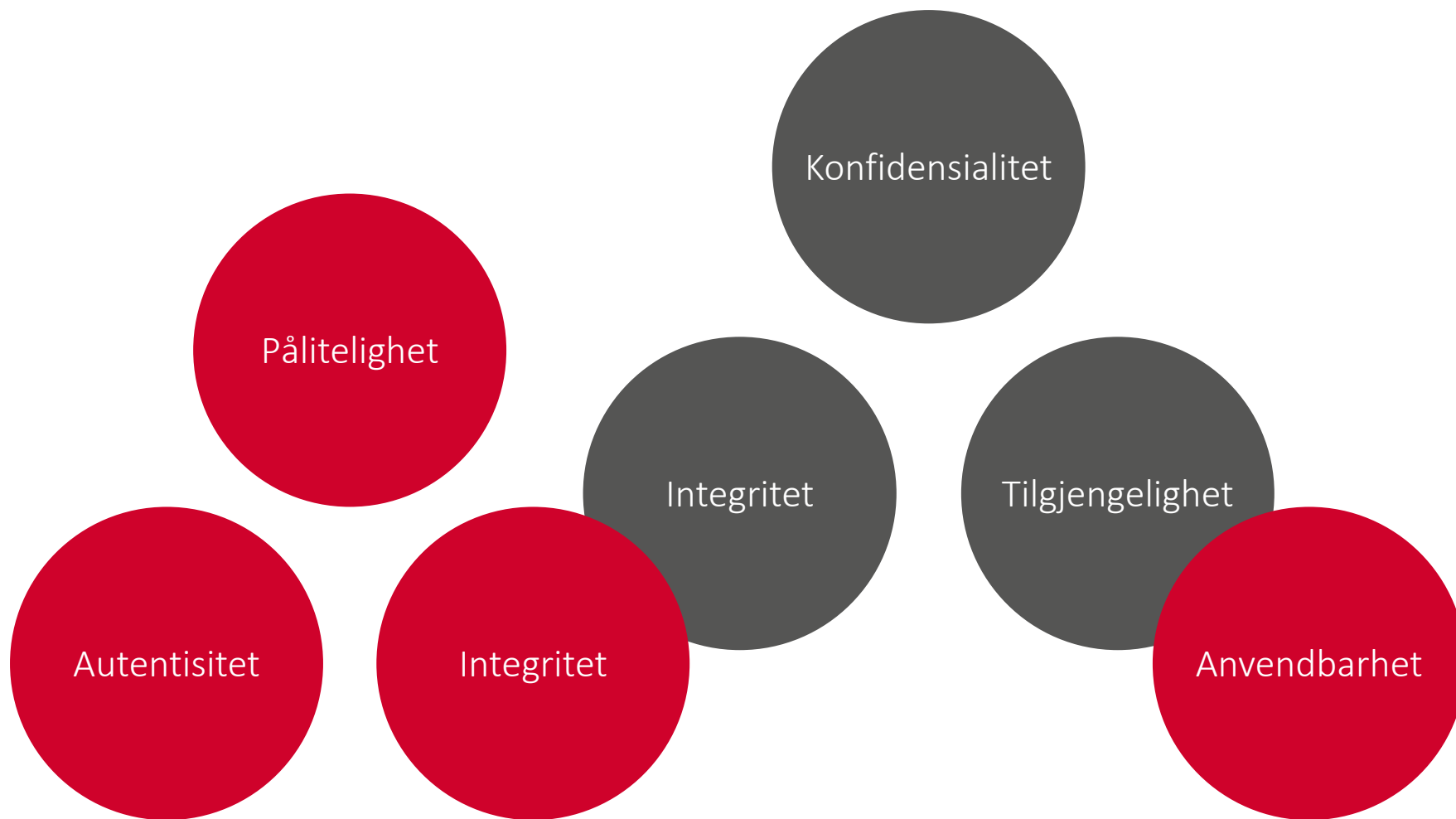
AUTENTISITET

Autentisk dokumentasjon er noe det kan bevises at

- den er hva den hevder å være,
- den er produsert eller sendt av den personen som hevder å ha produsert eller sendt den, og
- den er produsert eller sendt på det påståtte tidspunktet.



Informasjonssikkerhet og dokumentasjonsforvaltning





Hvorfor skal IKT-sikkerhetsutvalget skal vurdere om det skal lages en IKT-sikkerhetslov i Norge?

- Tyskland har implementert IKT-sikkerhetslovgivning
- Fordi man tenker at lover faktisk får til endringer. Bare se hvordan GDPR har fått folk til endre oppførsel
- NIS Direktivet (The Directive on security of network and information systems) er det man vurderer å implementere som IKT sikkerhetslov



NIS-direktivet



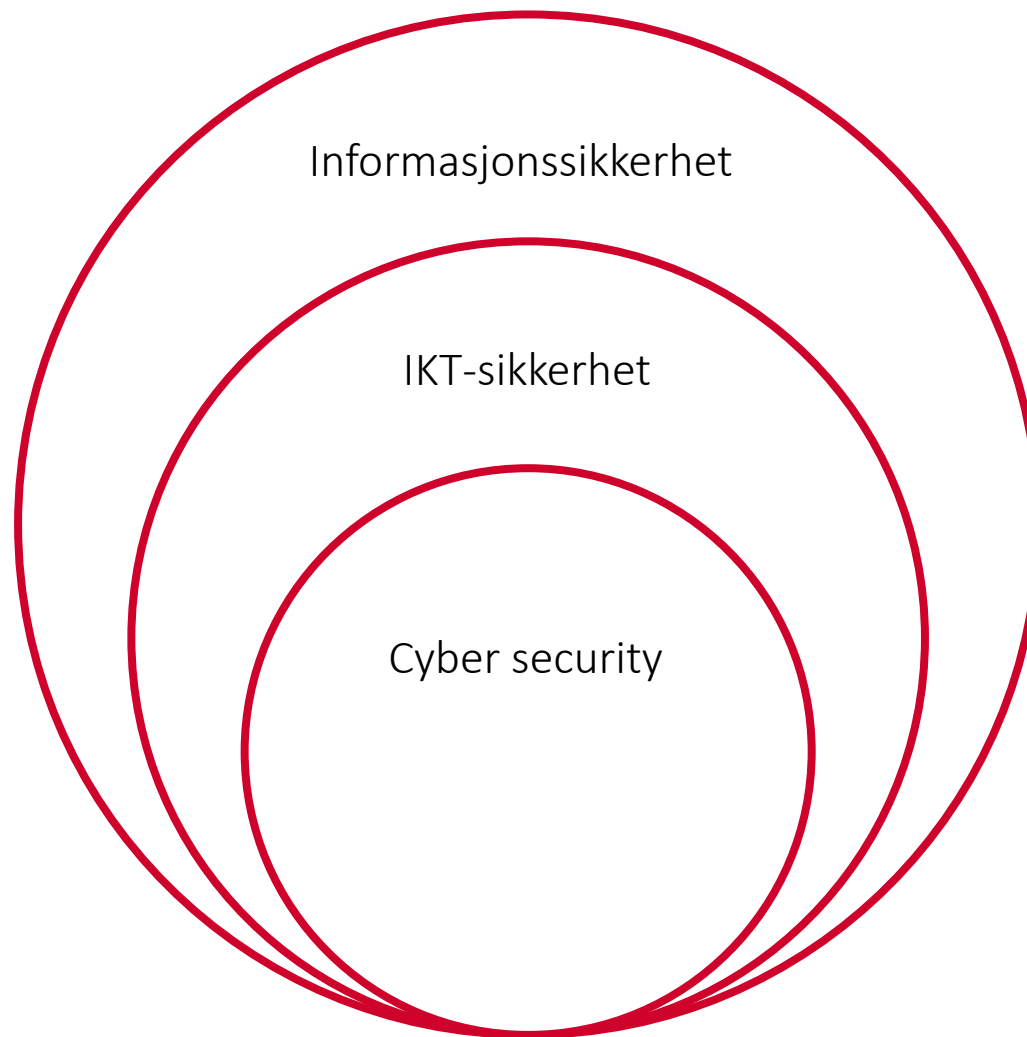
NIS direktivet setter opp juridiske krav for å forbedre den overordnede IKT-sikkerheten i EU/EØS ved å sikre:

- At medlemslandene har riktige ressurser - Computer Security Incident Response Team (CSIRT) og en nasjonal NIS-myndighet,
- Samarbeid mellom medlemslandene for strategisk samarbeid, informasjonsdeling og et team som kan reagere ved akutte hendelser
- En sikkerhetskultur på tvers av samfunnskritiske bransjer som lener seg kraftig på IKT slikt som energi, transport, vann, bank, finans, helse og digital infrastruktur

<https://ec.europa.eu/digital-single-market/en/network-and-information-security-nis-directive>



Informasjonssikkerhet





Hvorfor holder det ikke at
IKT-avdelingen sysler med
IKT-sikkerhet?

A faint, light gray world map is visible in the background, centered behind the text.

**I'en i IKT er informasjon
og informasjon er vi jo
opptatt av!**



Lagring av informasjons gjøres i mange løsninger



- Filstruktur
- SharePoint
- Fagsystem
- Ulike soner og plattformer
- Sak-/arkivløsning
- Arkivkjerne
- Historiske databaser



Det gjøres mye informasjonsforvaltning i skytjenester



- Sak-/arkivløsning SaaS
- Office 365
- Prosjektrom



Integritet, konfidensialitet og tilgjengelighet er vanskelig på tvers - Integrasjoner



- SaaS
- SharePoint
- Fagsystem
- Ulike soner og plattformer
- Sak-/arkivløsning
- Arkivkjerne
- Historiske databaser



Tilgangsstyring er noe av det viktigste i IKT-sikkerhet



- Tilgangsstyring i sak-/arkiv
- Tilgangsstyring på tvers
- Automatisert tilgangsstyring

A faint, light gray world map is visible in the background, centered behind the text.

**Det er vanskelig å
bedømme risiko i en
teknologisk verden**



Hvordan kan IKT-sikkerhet
bli inkludert i arkivplanen?



Hva er Nasjonal sikkerhetsmyndighets grunnprinsipper for IKT-sikkerhet?

- NSMs grunnprinsipper for IKT-sikkerhet definerer et sett med prinsipper for hvordan IKT-systemer bør sikres for å beskytte verdier og leveranser.
- Grunnprinsippene beskriver hva en virksomhet bør gjøre for å sikre et IKT-system.
- De beskriver også hvorfor det bør gjøres, men ikke hvordan. Grunnprinsippene kompletterer, men erstatter ikke en virksomhets sikkerhetsstyringsarbeid.

Kilde:

https://www.nsm.stat.no/globalassets/dokumenter/nsm_grunnprinsipper_ikt-sikkerhet_enkeltside_3008.pdf





Hva er viktig for IKT-sikkerhet i en arkivplan?

1. Innledning

- 1.1 Bakgrunn og formål
- 1.2 Oppdatering av arkivplan
- 1.3 Vedtatt arkivplan

2. Organisasjon

- 2.1 Om virksomheten
- 2.2 Om ansvar og myndighet
- 2.3 Organisering av dokumentasjonsforvaltningen
- 2.4 Arkivtjenestens oppgaver

3. Lover og overordnede retningslinjer

- 3.1 Lover og forskrifter
- 3.2 Instrukser og overordnede retningslinjer

4. Rutiner og retningslinjer for virksomhetens arkivtjeneste

- 4.1 Egenutviklede bestemmelser, instrukser og rutiner
- 4.2 Andre rutiner

5. Oversikt arkivbeholdning og informasjonsarkitektur

- 5.1 Fremfinningssystem
- 5.2 Arkivavgrensing
- 5.3 Bestandsoversikt

6. Dokumentasjonskrav

- 6.1 Dokumentasjonskrav til virksomheten
- 6.2 Overholdelse av dokumentasjonskrav
- 6.3 Restanse og kontroll

7. Bevaring og kassasjon

- 7.1 Bevarings- og kassasjonsbestemmelser for virksomheten
- 7.2 Ansvar for bevaring- og kassasjon

8. Avlevering og periodisering

- 8.1 Avleveringsplaner
- 8.2 Periodiseringsplaner

9. Avtaler med eksterne og rutiner for oppfølging

- 9.1 Avtaler med eksterne
- 9.2 Rutiner for oppfølging av avtalene

10. Informasjonssikkerhet

- 10.1 Overordnet ansvar
- 10.2 Dokumentsikkerhet
- 10.3 Nødrutiner

11. Opplæring og kompetanse

- 11.1 Opplæring av andre
- 11.2 Kompetanseheving for arkivtjenesten

12. Risikohåndtering og tiltak

- 12.1 Risiko, mangler og tiltak
- 12.2 Rutiner og retningslinjer som mangler



Hvor er IKT-sikkerhet viktig?

1. Innledning

- 1.1 Bakgrunn og formål
- 1.2 Oppdatering av arkivplan
- 1.3 Vedtatt arkivplan

2. Organisasjon

- 2.1 Om virksomheten
- 2.2 Om ansvar og myndighet
- 2.3 Organisering av dokumentasjonsforvaltningen
- 2.4 Arkivtjenestens oppgaver

3. Lover og overordnede retningslinjer

- 3.1 Lover og forskrifter
- 3.2 Instrukser og overordnede retningslinjer

4. Rutiner og retningslinjer for virksomhetens arkivtjeneste

- 4.1 Egenutviklede bestemmelser, instrukser og rutiner
- 4.2 Andre rutiner

5. Oversikt arkivbeholdning og informasjonsarkitektur

- 5.1 Fremfinningsplan
- 5.2 Arkivbeholdning
- 5.3 Bestemmelse

Konfidensialitet

Tilgjengelighet

6. Dokumentasjonskrav

- 6.1 Dokumentasjonskrav til virksomheten
- 6.2 Overholdelse av dokumentasjonskrav
- 6.3 Restanse og kontroll

Integritet

7. Bevaring og kassasjon

- 7.1 Bevarings- og kassasjonsbestemmelser for virksomheten
- 7.2 Ansvar for bevaring- og kassasjon

8. Avlevering og periodisering

- 8.1 Avleveringsplaner
- 8.2 Periodiseringsplaner

9. Avtaler med eksterne og rutiner for oppfølging

- 9.1 Avtaler med eksterne
- 9.2 Rutiner for oppfølging av avtaler

10. Informasjonssikkerhet

- 10.1 Overordnet ansvar
- 10.2 Dokumentsikkerhet
- 10.3 Nødrutiner

Konfidensialitet

Integritet

Tilgjengelighet

11. Opplæring og kompetanse

- 11.1 Opplæring av andre
- 11.2 Kompetanseheving for arkivtjenesten

12. Risikohåndtering og tiltak

- 12.1 Risiko, mangler og tiltak
- 12.2 Rutiner og retningslinjer for håndtering av mangler

Konfidensialitet

Integritet

Tilgjengelighet



Hva må en arkivar være opptatt av når det gjelder IKT-sikkerhet?



- Tilgangsstyring
 - Arkivarer må ta den gamle skrankevokter rollen inn i den digitale tidsalder
- Lagringsplasser
 - Arkivarer må se på forvaltningen av alle informasjonslagringsplasser – i og utenfor sak-/arkiv, aktive og historiske
- Skytjenester
 - Arkivarer må vite hva skytjenester er og hva de bør og ikke bør brukes til
- Risikovurdering
 - Arkivarer må sette seg inn i det nye risikobildet som gjelder digitalt informasjonsforvaltning

Takk for oppmerksomheten!

Kristine Synnøve Brorson,
Senior Consulting Manager
E-post: kristine.brorson@soprasteria.com
Mobil: 951 80 085

sopra  steria

Delivering Transformation. Together.

www.soprasteria.no