

Lärlabb C

Informationshantering

Syfte: Detta lärlabb fokuserar på informationshantering på ett lekfullt sätt och hur kan skapa ett grundtänk kring informationshantering för sig själv och sina medarbetare. Det är ett stöd i att leda arbetet på den digitala arbetsplatsen.



Välkommen!



Agenda för de kommande 55 minuterna

Introduktion i informationshantering

Bingo

Informationssäkerhet och lagar

Reflektioner i grupper

Pannelsamtal om informationshantering med Joakim Lindström
(Skellefteå kommun) Mats Johansson (RV) Thomas Häggström (Umeå
kommun)

Avslutning



Informationshantering och Informationssäkerhet

- Informationshantering handlar om att samla in, lagra, bearbeta och dela information på ett strukturerat sätt.
- Informationssäkerhet syftar till att skydda information från obehörig åtkomst, förlust eller manipulation.
- Offentlig verksamhet hanterar ofta känsliga personuppgifter och måste följa strikta lagkrav.

Check-in: Varför är detta viktigt för chefer och ledare?



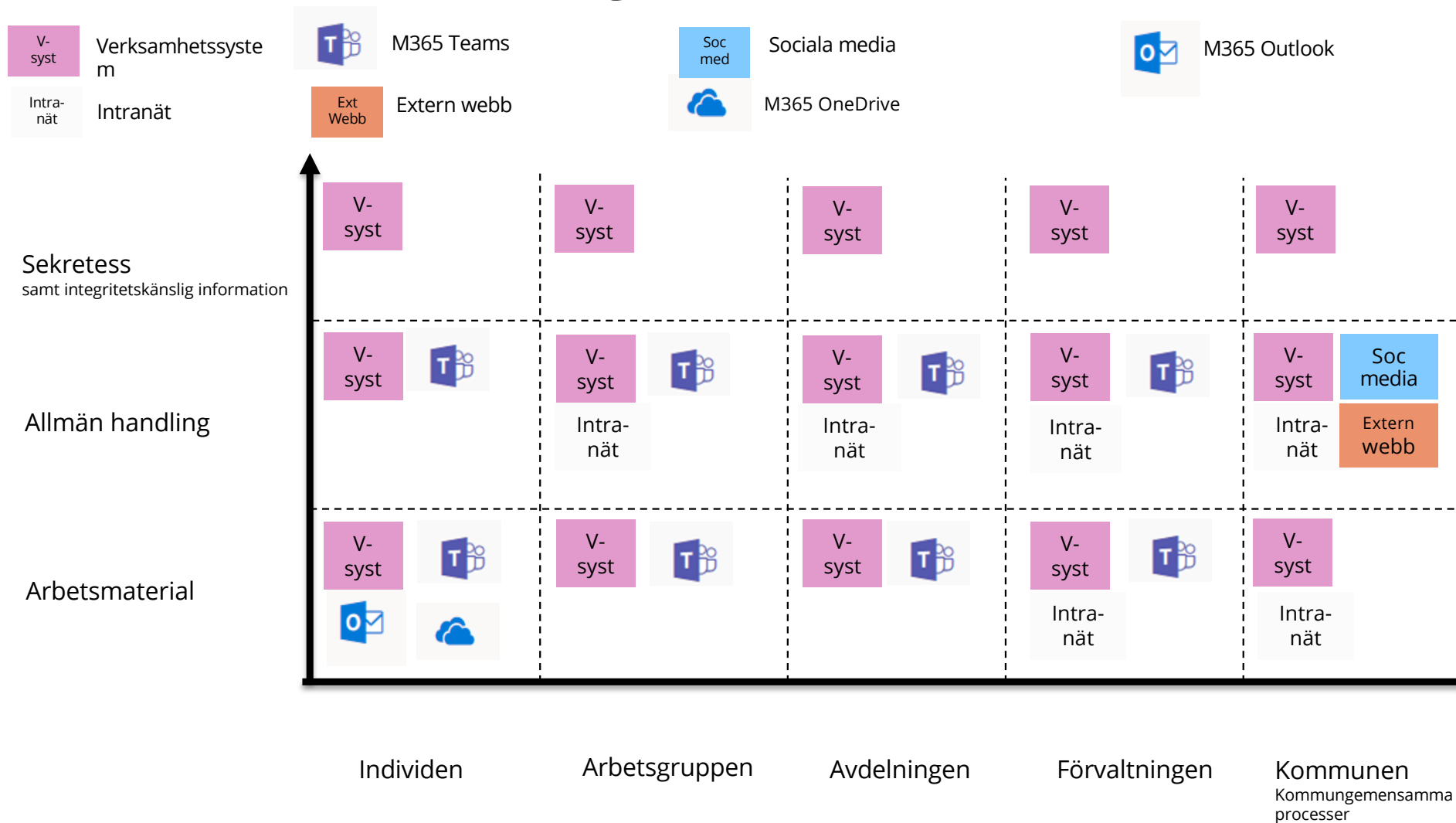
Informationshantering - varför är det viktigt?

Vilka faktorer påverkar hur information hanteras?

- Vilken typ av information är det? Anteckningar? Policy? Sekretessbelagd information? Offentlig handling? Annat?
- Vilket är det faktiska innehållet - text, bild mm
- Vilket format? Digitalt – vilket digitalt format? Papper? Format som passar för delning/samarbete?
- Var lagras informationen? Arkiv? Pärm? Filsystem? Teams? Annat verksamhetsnära system? System som passar för delning/samarbete?
 - Dokumentnamn, metadata etc



Informationshantering



Informationshanterings-

5 min eget labbande



Lagstiftning som Reglerar Informationshantering i Offentlig Verksamhet

- GDPR (Dataskyddsförordningen)
- Offentlighetsprincipen och Tryckfrihetsförordningen
- Arkivlagen (1990:782)
- Säkerhetsskyddslagen (2018:585)



AI- och Molntjänster

Schrems II och tredjelandsoverföring

- **Schrems II-domen** innebär att överföring av personuppgifter till USA (eller andra länder utanför EU/EES) endast är tillåten om det finns **adekvata skyddsåtgärder**.
- Om AI/Moln-tjänsten drivs av ett amerikanskt företag kan den omfattas av amerikanska lagar som **Cloud Act**, vilket kan medföra risk för obehörig åtkomst.
- Kontrollera om tjänsten har implementerat **EU:s standardavtalsklausuler (SCCs)** eller om **EU-U.S. Data Privacy Framework** gäller.



AI- och Molntjänster

- Amerikanska företag som Microsoft, Google och Amazon kan tvingas lämna ut data lagrad på EU-servrar till amerikanska myndigheter, vilket kan stå i konflikt med GDPR och orsaka överföring av data till USA utan användarnas vetskap.
- För att minimera riskerna väljer vissa företag EU-baserade molntjänster eller kryptering. Svenska myndigheter kan använda amerikanska molntjänster om nödvändiga åtgärder vidtas för att säkerställa GDPR-efterlevnad, inklusive överföring av personuppgifter till tredje land, skyddsåtgärder, konsekvensbedömningar och förhandlingar med leverantörer.

Diskutera/fundera på:

1. Riskanalys inom informationssäkerhet

➡ **Fråga:** Vilka är de största riskerna i er organisation när det gäller hantering av känslig information?

Diskussion: Identifiera risker såsom obehörig åtkomst, bristande efterlevnad av GDPR eller otillräcklig säkerhetsmedvetenhet bland personal. Hur kan dessa risker minimeras?

2. Offentlighetsprincipen vs. informationssäkerhet

➡ **Fråga:** Hur balanserar ni öppenhet och transparens med behovet av informationssäkerhet och sekretess?

Diskussion: Offentlighetsprincipen kräver att information är tillgänglig, men vissa uppgifter måste skyddas. Hur arbetar ni med att avgöra vad som ska vara offentligt och vad som ska sekretessbeläggas?

3. Strategier för GDPR-efterlevnad

➡ **Fråga:** Hur säkerställer ni att er organisation följer GDPR och andra lagkrav i praktiken?

Diskussion: Vilka processer och verktyg har ni på plats för att hantera personuppgifter på ett lagligt och effektivt sätt? Finns det brister i dagens hantering som behöver åtgärdas?

4. Digitalisering och framtidens informationshantering

➡ **Fråga:** Hur påverkar digitalisering och AI er hantering av information och säkerhet?

Diskussion: Vilka digitala lösningar använder ni idag? Finns det områden där automatisering eller AI kan förbättra säkerhet och effektivitet i informationshanteringen?

5. Ledarskapets roll i informationssäkerhet

➡ **Fråga:** Vilket ansvar har ledare och chefer i att bygga en stark säkerhetskultur?

Diskussion: Hur kan chefer och ledare arbeta för att öka medvetenheten om informationssäkerhet? Vilka åtgärder kan införas för att förbättra säkerhetsrutiner och efterlevnad?



Reflektioner i grupper

5&5

10 minuter



Diskutera/fundera på:

1. Riskanalys inom informationssäkerhet

➡ **Fråga:** Vilka är de största riskerna i er organisation när det gäller hantering av känslig information?

Diskussion: Identifiera risker såsom obehörig åtkomst, bristande efterlevnad av GDPR eller otillräcklig säkerhetsmedvetenhet bland personal. Hur kan dessa risker minimeras?

2. Offentlighetsprincipen vs. informationssäkerhet

➡ **Fråga:** Hur balanserar ni öppenhet och transparens med behovet av informationssäkerhet och sekretess?

Diskussion: Offentlighetsprincipen kräver att information är tillgänglig, men vissa uppgifter måste skyddas. Hur arbetar ni med att avgöra vad som ska vara offentligt och vad som ska sekretessbeläggas?

3. Strategier för GDPR-efterlevnad

➡ **Fråga:** Hur säkerställer ni att er organisation följer GDPR och andra lagkrav i praktiken?

Diskussion: Vilka processer och verktyg har ni på plats för att hantera personuppgifter på ett lagligt och effektivt sätt? Finns det brister i dagens hantering som behöver åtgärdas?

4. Digitalisering och framtidens informationshantering

➡ **Fråga:** Hur påverkar digitalisering och AI er hantering av information och säkerhet?

Diskussion: Vilka digitala lösningar använder ni idag? Finns det områden där automatisering eller AI kan förbättra säkerhet och effektivitet i informationshanteringen?

5. Ledarskapets roll i informationssäkerhet

➡ **Fråga:** Vilket ansvar har ledare och chefer i att bygga en stark säkerhetskultur?

Diskussion: Hur kan chefer och ledare arbeta för att öka medvetenheten om informationssäkerhet? Vilka åtgärder kan införas för att förbättra säkerhetsrutiner och efterlevnad?



Pannelsamtal om informationshantering

Joakim Lindgren, Skellefteå Kommun

Mats Johansson, Region Västerbotten

Thomas Häggström, Umeå Kommun

Moderator: Malin Bergvall, Region Västerbotten



Sammanfattning

Tips på personer att fråga för stöd kring informationshantering i din organisation:

- Nämndsekreterare/Sekretariat/Arkivarie
- Informationssäkerhetsansvarig/Dataskyddsansvarig
- Informationsarkitekt/informationscontroller
- Personuppgiftsansvarig
- M365 ambassadörer/personer som arbetar med digitala arbetssätt



[Översikt](#)[Mina kurser](#)[Tema 5: Lärlabb](#)[Introduktion](#)[Introduktion](#)[A: Kreativa funktioner i M365](#)[B: AI som stöd i din arbetsvardag](#)[C: Informationshanteringsbingo](#)[D: Canvas för din verksamhet](#)[E: Omvärldsspaning Robotar](#)[F: Vandra i kundens digitala skor](#)[G: Antipilot - testa "sluta göra"](#)[Extra: Hitta fejkmailen](#)[Självstudier](#)

Introduktion



Nyheter

Syfte

Syftet med detta temaområde är att du får möjlighet att utforska, testa och träna på nya digitala verktyg och metoder som underlättar, stödjer, ökar kvaliteten på att arbeta och leda digitalt.

Kunskapsmål

Efter genomgången temaområde kommer du att ha

- ökad erfarenhet av att arbeta digitalt
- ökad erfarenhet av att leda digitalt
- ökad kunskap om metoder att leda digitalt förändringsarbete

Sugen på
lärlabb? Då ses
vi 21 mars 9-10

Tack!