UNIVERSITY OF OSLO

Sikkerhetspolicies som normative virkemidler for å oppnå informasjonssikkerhet

Tobias Mahler
Stipendiat
Senter for rettsinformatikk, UiO

Agenda

- Definisjoner
- Strategi eller instruks?
- Et instrumentelt perspektiv på informasjonssikkerhet
- Policy som normativt virkemiddel
- Juridiske krav til sikkerhetspolicies

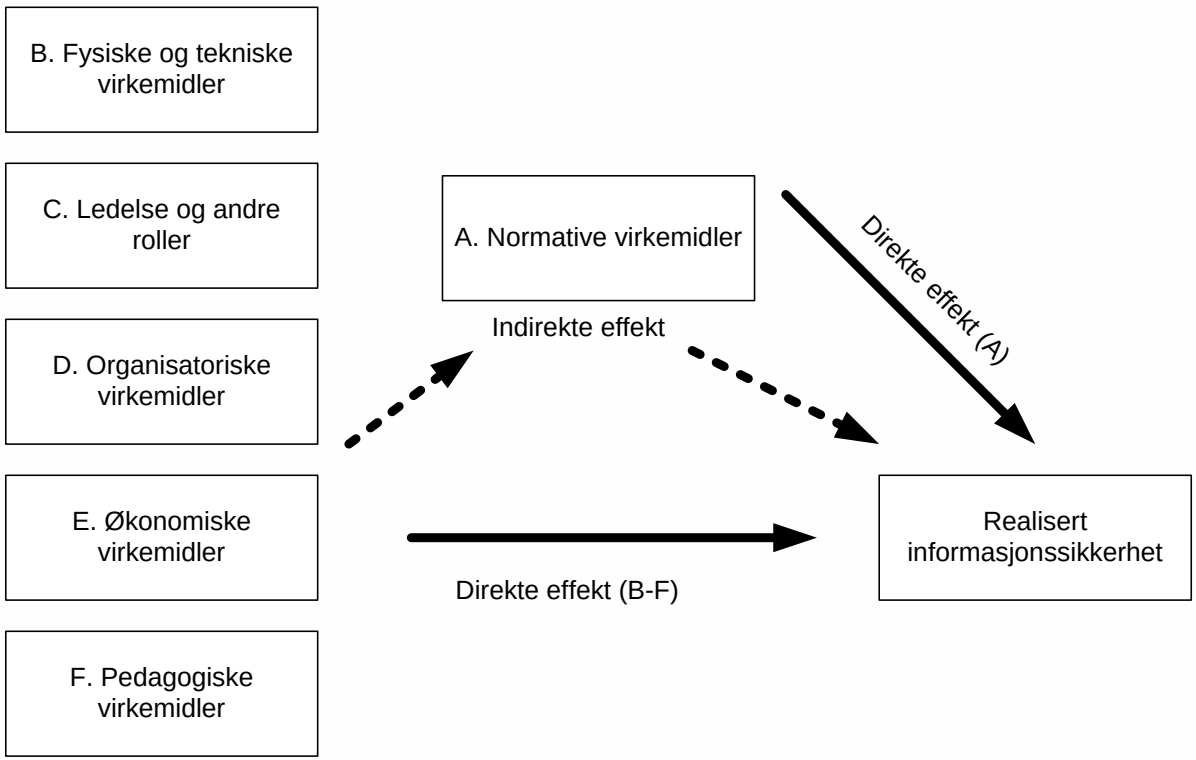
Definisjoner av “security policy”

- The set of **laws, rules, and practices** that regulate how an organization manages, protects, and distributes sensitive information. michigan.gov
- A security policy is a set of **basic rules** applied to all network users. network-security.adopto-computers.com
- A security policy is the set of **rules, principles, and practices** that determine how security is implemented in an organization. slis-two.lis.fsu.edu
- The set of management statements that documents an organization's philosophy of protecting its computing and information assets, or the set of **security rules** enforced by the system's security features. austin.cc.tx.us
- A security policy is a plan of action for tackling security issues, or a **set of regulations** for maintaining a certain level of security. wikipedia.org

Sikkerhetspolicy: strategi eller instruks

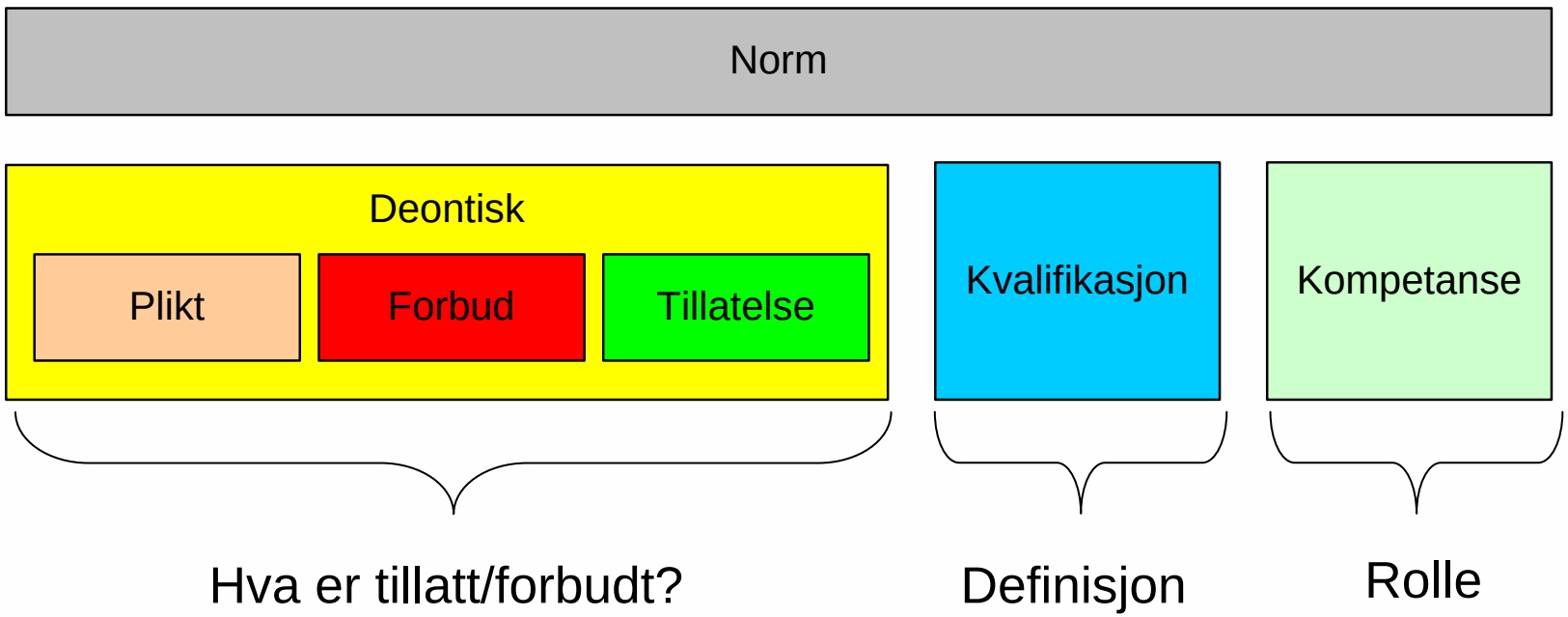
- Sikkerhetsstrategi
  - Ikke bindende, antagelig sjelden rettslig relevans
- Sikkerhetsinstruks
  - Internt bindende, kan ha rettslig relevans
- Begge bør baseres på risikoanalyser
  - Hva kan skje og hvordan kan det unngås
  - Hvilke rettslige følger vil en uønsket hendelse ha?
  - Kost-nytte-vurderinger

Informasjonssikkerhet – et instrumentelt syn på rettslige reguleringer (Haug 2006)



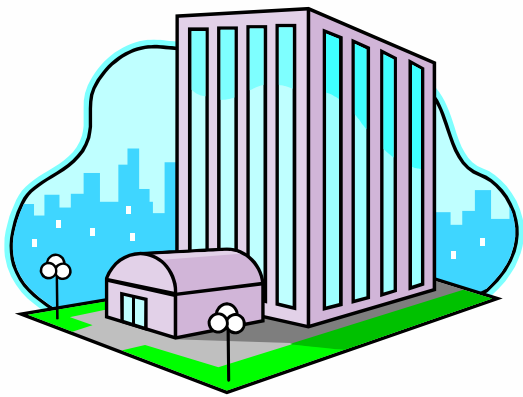
Are Vegard Haug: Rettslige reguleringer av informasjonssikkerhet, COMPLEX 2/06, Oslo 2006, s. 17.

Policy som normativt virkemiddel



Juridiske krav til sikkerhetspolicies

- For virksomheten: Informasjonssikkerhet
  - Personopplysningsloven + forskriften
  - Forretningshemmeligheter
  - Spesialregler
    - Offentlig sektor
    - Finanssektoren (IKT forskriften)
    - Helseopplysninger
    - Gradert informasjon (sikkerhetsloven m/ forskrifter)
    - Elektronisk signatur
  - Kontrakter



- For ansatte:
  - Arbeidsrett
  - Strafferett

Avsluttende kommentarer

- Håndhevelse
  - Den rettslige håndhevelsen er begrenset
  - Håndhevelsen må primært skje gjennom andre virkemidler
    - Pedagogiske og organisatoriske virkemidler
- Rettslige krav til innhold og intern håndhevelse
  - Offentligrettslige krav
  - Privatrettslige krav
- Integrere rettslige aspekter i risikoanalyser
  - Avklare behov for sikkerhetsnivået
  - En misforståelse av rettslige krav kan bidra til et “for høyt sikkerhetsnivå”, som begrenser andre aktiviteter

UNIVERSITY OF OSLO

Takk for oppmerksomheten!

- Tobias Mahler
- Senter for rettsinformatikk, UiO
- http://folk.uio.no/tobiasm/