

**Printerløsninger over ulike nettverkssoner**

Målgruppe Dette temaarket er spesielt relevant for:	<input checked="" type="checkbox"/> Leverandør <input checked="" type="checkbox"/> IKT-ansvarlig <input type="checkbox"/> Prosjektleder	<input checked="" type="checkbox"/> Sikkerhetsleder/koordinator <input type="checkbox"/> Virksomhetens leder/ledelse <input type="checkbox"/> Medarbeider/ansatt	<input checked="" type="checkbox"/> Databehandler <input type="checkbox"/> Personvernombud <input type="checkbox"/> Annet, spesifiser
Ansvar	IKT-Ansvarlig		
Når	Under etablering av et informasjonssystem eller ved endringer		
Formål	Beskrive behovet for å kontrollere nettverkskommunikasjon mellom soner ved felles utskriftløsninger		
Omfang	Omfatter all nettverkskommunikasjon innenfor et informasjonssystem		
Hjemmel	Personopplysningsforskriften §§ 2-7, 2-11 og 2-13		
Referanser	Veileder i sikkerhetsarkitektur: Systemteknisk sikkerhet – Sikkerhetsbarrierer Systemteknisk sikkerhet - Datakommunikasjon		

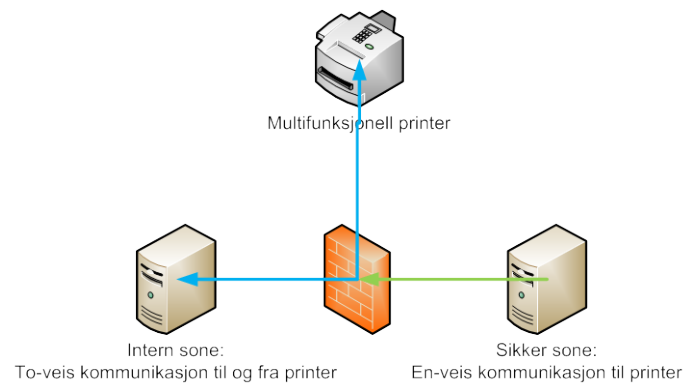
Bakgrunn

Av økonomiske årsaker, brukeropplæring og kontroll på utskrifter velger flere virksomheter å minimalisere antallet skrivere ved å slå sammen funksjonalitet i en og samme printerløsning.

Slike printerløsninger har ulike innebygde tjenester som eksempelvis ftp, webservere og faks. Det er også mulig å ha flere nettverkskort i printer, som igjen gjør det attraktivt å benytte en slik løsning felles for ulike nettverkssoner. Dette innebærer også behandling av personopplysninger av ulik beskyttelsesgrad i de fleste tilfeller, både alminnelige og sensitive.

For at nevnte løsninger skal fungere etter hensikten må de kobles opp mot ulike nettverkssoner, og det innebærer som oftest to ulike nettverkskabler som settes i hver sin sone. En slik tilnærming vil normalt omgå den oppsatte sikkerhetsbarrieren mellom sonene, og dermed gjøre at den opprinnelige funksjonen omgås. De nevnte tjenestene og at løsningen skal håndtere ulike grader av personopplysninger gjør den til et risikomoment uten særlige sikkerhetstiltak.

Nr.	Aktivitet/Beskrivelse
1	Printerløsninger over ulike soner <ul style="list-style-type: none"> Printerkommunikasjon bør styres gjennom brannmur og løsningen bør derfor stå i DMZ på sikkerhetsbarriere Antall kommunikasjonsporer i sikkerhetsbarrierer må holdes til et absolutt minimum Printerløsningen må konfigureres slik at tilgjengelige tjenester ikke øker risikoen for at personopplysninger havner på avveie eller på annen måte kompromitteres. Datakommunikasjonen må initieres fra sikre soner for å forhindre uautorisert trafikk inn i slike soner. To nettverkskort i en printer vil gjøre at sikkerhetsbarrieren i praksis blir omgått og sikkerheten mellom to ulike soner ligger i selve printeren.
2	Mulige metoder <ul style="list-style-type: none"> Styring av kommunikasjon mellom printerserver og printerløsning – Enveiskommunikasjon er å foretrekke. Printerløsningen bør benytte kryptering av lagringsenheter for å ivareta konfidensialitet. Nødvendig tilgangsstyring til printerløsningen må etableres for at utskrifter ikke kommer på avveie Gode rutiner for avhending av brukt utstyr for å hindre uautorisert utlevering bør etableres



Figur 1: Felles printerløsning mellom ulike soner