

**Bruk av terminalserver**

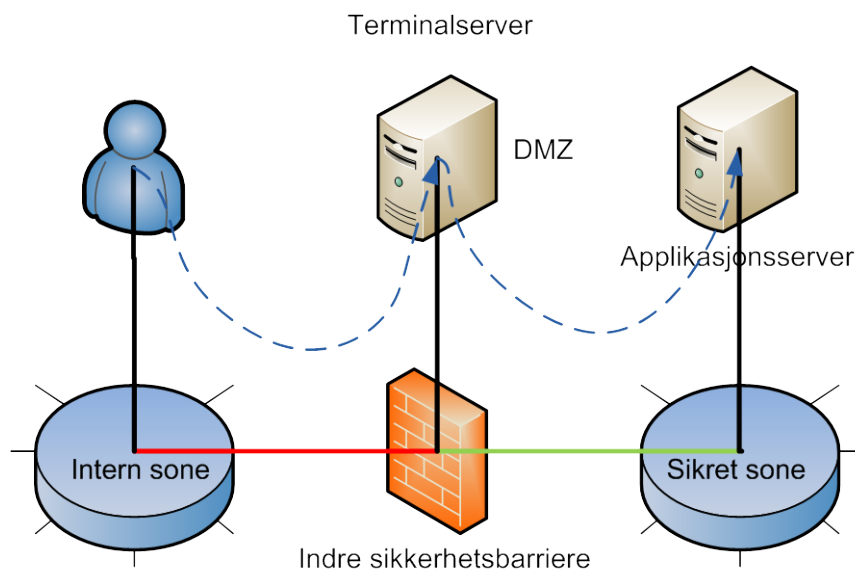
Målgruppe Dette temaarket er spesielt relevant for:	<input checked="" type="checkbox"/> Leverandør <input checked="" type="checkbox"/> IKT-ansvarlig <input type="checkbox"/> Prosjektleder	<input checked="" type="checkbox"/> Sikkerhetsleder/koordinator <input type="checkbox"/> Virksomhetens leder/ledelse <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 bruk av terminalserver for tilgang til sikrede soner		
Omfang	Beskrive bruk av terminalserver for tilgangsstyring mellom nettverksoner hvor personopplysninger behandles og tilgang fra eksterne soner inn mot virksomhetens informasjonssystem.		
Hjemmel	Personopplysningsforskriften §§ 2-7, 2-11 og 2-13		
Referanser	Ingen		

Bakgrunn

For å styre tilgang til sikrede soner hvor sensitive personopplysninger behandles og for å ivareta nødvendig konfidensialitet må tekniske tiltak etableres. En terminalserver eller lignende teknologi vil kunne styre hvem som har tilgang til bestemte soner og samtidig hindre at informasjon flyter ukontrollert mellom de ulike sonene. En terminalserver plasseres normalt i en DMZ på sikkerhetsbarrieren mellom de ulike sonene, som vist i figuren på siste side. En godt konfigurert terminalserver-løsning gjør at en kan ha ulike sikkerhetsnivå i samme nettverksstruktur/informasjonssystem.

Nr.	Aktivitet/Beskrivelse
1	<p>Terminalserveren og sikkerhetsbarrierene kombinert må ivareta noen grunnleggende prinsipper for at sikkerheten for de ulike sonene skal ivaretas på en tilstrekkelig måte. Disse er:</p> <ul style="list-style-type: none"> • Plassering av terminal-server i DMZ i figur 1. • Hindre klipp og lim • Hindre filoverføring • Behovsstyrt tilgangsstyring • Kun åpne for nødvendige kommunikasjonsporter i sikkerhetsbarriere, begrense hvilken vei kommunikasjonen kan gå og mellom hvilke enheter. Påse at ingen kommunikasjon som kan påvirke informasjonssikkerheten flyter direkte mellom soner. • Se temaark om nettverkskommunikasjon for informasjon om autentiseringsløsninger og nettverkskommunikasjon.
2	<ul style="list-style-type: none"> • En terminalserver eller lignende teknologi kan også benyttes sammen med andre sikkerhetsbarrierer for å styre tilgang til soner. Dette kan for eksempel være ved pålogging fra eksterne soner (Internett) mot virksomhetens informasjonssystem. Virksomheten kan da få bedre kontroll med informasjonsflyten inn og ut av virksomheten, og med rimelighet kunne forvisse seg om hvor informasjon befinner seg.

Nr.	Aktivitet/Beskrivelse
	<ul style="list-style-type: none"> • Ekstern kommunikasjon til en terminalserver bør krypteres over nettverk hvor virksomheten ikke har konfigurasjonskontroll. • Utstyr som kobles opp mot terminalserveren fra eksterne nettverk bør være under virksomhetens konfigurasjonskontroll eller at det med rimelighet forvisses at utstyr som kobler seg opp har tilfredsstillende sikkerhet etablert. Eksempelvis vha. network access control el. • Virksomheten bør også forvise seg om at det er rett person som autentiserer seg inn mot virksomhetens informasjonssystem fra eksterne nettverk. Eksempelvis via en 2-faktor løsning.



Figur 1: Bruk av terminalserver for tilgang til sikrede nettverkssoner