«White paper» om informasjonssikkerhet

# Nettverkssikkerhet

## Beskyttelse av nettverksenheter på kontoret

www.sharp.no

SHARP
Be Original.

# Innhold

# Innledning

## I dagens tilkoblede samfunn er effektiv informasjonssikkerhet i hele bedriftsnettverket viktigere enn noensinne.

Vi ser hver dag utallige ondsinnede forsøk på å stjele, manipulere eller spre konfidensielle dokumenter, eller skaffe seg uautorisert tilgang til private nettverk og bedriftsnettverk. I dette «white paper» dokumentet undersøker vi de største utfordringene som bedriftene står overfor når det gjelder å beskytte den delen av IT-infrastrukturen som består av nettverkstilkoblede kontorenheter som blant annet multifunksjonsskrivere (MFP) og vanlige skrivere.

I dette «white paper» dokumentet ser vi på følgende:

- **Bakgrunnen**
  Alle bedrifter står overfor utfordringer når det gjelder nettverkssikkerhet og nettverkstilkoblede (multifunksjons)skrivere er sårbare punkter som ofte overses. Hackere og cyberkriminelle bruker dem som inngangsportal for å stjele konfidensielle data som er lagret på harddisker og andre nettverkstilkoblede enheter, gjøre skade og ødelegge forretningsdriften. Dette kan få alvorlige konsekvenser for produktivitet og lønnsomhet.

- **Problemet**
  Risikoen som usikrede (multifunksjons)skrivere utgjør, blir ofte misforstått eller oversett. I mange tilfeller mangler bedriftene dessuten kompetansen og ressursene som trengs for å takle problemet. Manglende bevissthet blant brukere gjør saken enda verre, ettersom dårlige rutiner øker faren for at dokumenter og data kompromitteres. Selv om bedriftene forstår hva som må gjøres for å få på plass retningslinjer for utskriftssikkerhet, kan prosessen være komplisert og tidkrevende.

- **Anbefalingene**
  Vi beskriver her ulike maskin- og programvareløsninger samt anbefalte fremgangsmåter som kan hjelpe deg å skape et trygt utskriftsmiljø og hindre at uvedkommende får tilgang til eller angriper bedriftens nettverkstilkoblede enheter. I dette avsnittet finner du konkrete svar på noen av de viktigste sikkerhetsutfordringene:

  - Seks trinn for å innføre og opprettholde standarder for utskriftssikkerhet ved hjelp av en kombinasjon av teknologi og optimaliserte programvareløsninger fra Sharp.
  - Innovative funksjoner og innstillinger som f.eks. passordbeskyttelse, overskriving av data og kryptering, som er tilgjengelige på alle nettverkstilkoblede Sharp-enheter i gjeldende serie.
  - Valgfrie løsninger som f.eks. Sharp Remote Device Manager (SRDM), som hjelper deg å utarbeide konsekvente retningslinjer for utskriftssikkerhet, og administrere skriverparken din på en enkel og effektiv måte.
  - Valgfrie avanserte (multifunksjons)skriverfunksjoner som f.eks. Data Security Kit (DSK).
  - Valgfrie tjenester som f.eks. sikkerhetsrevisjon, sikkerhet som tjeneste og sletting av data ved leasingslutt, som er tilgjengelige gjennom Sharp direct-kanalen.

- **Konklusjonen**
  Vi gir en oppsummering av følgende:

  - Funn av sårbarheter knyttet til de enkelte nettverkstilkoblede (multifunksjons)skriverne.
  - Våre anbefalinger basert på de integrerte Sharp-funksjonene og ytterligere sikkerhetsløsninger fra Sharp
  - De neste trinnene som er nødvendige for å utarbeide retningslinjer for utskriftssikkerhet – enten det gjøres internt eller med eksperthjelp fra Sharps profesjonelle serviceteam.

# Bakgrunn

## Selv om behovet for effektiv IT-sikkerhet har fått langt større oppmerksomhet de siste årene, har ett sentralt område farlig nok blitt glemt.

De fleste sikkerhetsbevisste organisasjoner sikrer nettverks- og dataressursene sine med den nyeste teknologien. Det innebærer blant annet bruk av brannmurer, krav om passordregler og brukergodkjenning, samt beskyttelse av krypterte og elektronisk signerte data.

Nye teknologier som f.eks. sky og mobil, har gitt IT-administratorer og sikkerhetsansvarlige ekstra utfordringer. Dagens intelligente (multifunksjons)skrivere har imidlertid mange funksjoner for nettverkskommunikasjon og datalagring. De har enkelt sagt utviklet seg til å bli kraftige, smarte datamaskiner. Ifølge IDC finnes det tett på 53 millioner skrivere og flerfunksjonsenheter i Vest- og Øst-Europa[1], og flertallet av disse er koblet til et nettverk. Som tilgangspunkter med IP-adresse er de like utsatt for skadelig programvare og hacker-angrep som en vanlig datamaskin eller et hvilket som helst annet nettverkstilkoblet endepunkt. Følgelig trenger de også de samme funksjonene for data-, kommunikasjons- og informasjonssikkerhet.

Via usikrede multifunksjonsskrivere vil hackere kunne ta seg inn gjennom ikke-kontrollerte porter og protokoller, og derfra få tilgang til sensitiv informasjon eller andre maskiner i nettverket. Kommunikasjon og data som er lagret på harddiskstasjonen eller i minnet til en multifunksjonsskriver, vil kunne fanges opp eller sendes uautorisert hvor som helst i verden. I tillegg vil de nettverkstilkoblede enhetene kunne utsettes for Denial of Service (DoS)-angrep der målet er å gjøre nettverksressursene utilgjengelige for sluttbrukerne. Dette vil da påvirke forretningsproduktiviteten. De kan også skape en åpen portal som gjør det mulig å spre virus eller drive nettfisking etter konfidensiell informasjon.

*25 % av IT-sikkerhetsbruddene som krevde iverksettelse av tiltak, involverte utskrifter.[2]*

Dette er på ingen måte skremselspropaganda – trusselen er svært reell. I en undersøkelse som IDC gjennomførte nylig, meldte 1 av 4 om betydelige IT-sikkerhetsbrudd som krevde iverksettelse av tiltak. I 25 % av tilfellene var utskrift involvert.[2]

Bedrifter som ikke beskytter (multifunksjons)skriverne sine, risikerer store skader samt tap av omdømme og kundetillit. Sikkerhetsbrudd kan få blant annet følgende konsekvenser:

- Tap av omsetning
- Tap av produktivitet på grunn av manglende data- og nettverkstilgang
- Tap av konkurranseevne på grunn av frastjålet informasjon
- Bøter på grunn av brudd på forskriftene
- Søksmål
- Uautorisert bruk av utstyr og nettverksressurser.

# Problem

## Hacker-aktiviteter og cyberangrep har blitt «normen», og utgjør en svært reell og umiddelbar trussel for bedrifter av alle slag og størrelser.

Det kommer kanskje som en overraskelse, men i en undersøkelse fra analyseinstituttet Quocirca innrømmet 63 % av de spurte bedriftene å ha opplevd ett eller flere utskriftsrelaterte brudd på persondatasikkerheten[3].

Hvorfor har da ikke bedriftene gjort mer for å bekjempe trusselen?

Den potensielle risikoen blir dessverre ofte oversett fordi man ikke er bevisst på hvilke sårbarheter som oppstår gjennom integreringen av enheter som (multifunksjons)skrivere i bedriftsnettverket. Det er derfor mange bedrifter som mangler eller har utilstrekkelige systemer og verktøy for utskriftssikkerhet – herunder skolert personale, beste praksis og sikkerhetsprosedyrer knyttet til bruk av nettverkstilkoblede enheter i bedriften. Alternativt kan det være at bedriften bruker enheter som i realiteten kun er beregnet på hjemmebruk og derfor har begrensede sikkerhetsfunksjoner.

Vi ser særlig at små og mellomstore bedrifter gjerne mangler tiltak for utskriftssikkerhet og/eller aldri har gjort en revisjon av utskriftssikkerheten. Større organisasjoner kan ha utilstrekkelige personalressurser eller kvalitetsverktøy til å måle, kontrollere og forebygge cyberangrep mot nettverksenheter og tilkoblede teknologier.

I tillegg kan dårlige rutiner blant brukerne være en betydelig utfordring for IT-administratorene og ofte forårsake store sikkerhetsproblemer for bedriften. Eksempler på slike dårlige rutiner kan være usikrede utskrifter, dokumenter som ligger ubevoktet i utmatingsskuffene på (multifunksjons)skriverne, utskrifter fra usikrede USB-stasjoner, utskrifter uten ende-til-ende-kryptering, eller lagring av sensitive dokumenter på (multifunksjons)skriverens harddisk.

Destrueringen av data etter endt kontrakt være et reelt problem.

*Nesten to tredjedeler av alle bedrifter har opplevd utskriftsrelaterte brudd på persondatasikkerheten.[3]*

Gjennom utskriftsprosessen kan en kopi av dataene som ble skrevet ut på enheten, bli lagret på harddisken på (multifunksjons)skriveren. Så hva skjer med dataene når kontrakten avsluttes?

Å sette opp et konsekvent nettverkssikkerhetssystem eller innføre retningslinjer for utskriftssikkerhet for å oppdage og forebygge uautorisert tilgang til en park av nettverkstilkoblede (multifunksjons)skrivere, kan dessverre være en svært komplisert og tidkrevende jobb. Du vil nesten garantert måtte gå gjennom følgende nøkkelfaser:

- Anslå og evaluere eventuelle potensielle implikasjoner ved det å ikke ha et nettverkssikkerhetssystem
- Gjenkjenne potensielle sårbarheter og hvordan disse kan skade nettverksinfrastrukturen
- Forstå kompleksiteten i utfordringen, som nødvendigvis vil variere fra bedrift til bedrift
- Finne en intern eller ekstern ressurs som kan hjelpe deg å takle utfordringen
- Identifisere verktøy som kan overvåke hele (multifunksjons)skriverparker, hindre uautorisert tilgang til nettverkstilkoblede ressurser og varsle deg om mistenkelig aktiviteter
- Konfigurere og drifte et pålitelig nettverkssikkerhetssystem som dekker alle de unike utfordringene bedriften din står overfor.

# Anbefalinger

## Hvis du nå kjenner at du begynner å bekymre deg for din egen nettverkssikkerhet, så ok! Risikoen som bedriften din er utsatt for, bør ikke undervurderes. Det er likevel ingen grunn til panikk.

Vi ønsker å vise deg hvordan du enkelt kan innføre omfattende tiltak for utskriftssikkerhet i bedriften din, og hvordan Sharp kan hjelpe deg å få innsikt i og skjerpe nettverkssikkerheten din uten noe stort hokus-pokus.

### Aktiver umiddelbar beskyttelse

Undersøkelser som bransjeanalytikere hos IDC har utført, viser at «leverandører av teknologi for papirbaserte utskrifter og dokumenttjenester jobber målrettet med å sikre utskriftsenhetene på en måte som hindrer at hackere kan få tilgang til bedriftsnettverk via utskriftsenhetene.»[4]. Like fullt er det mange bedrifter som overser eller ikke konfigurerer sikkerhetsinnstillingene sine riktig, og dette kan gjøre dem sårbare for angrep.

Sikkerhetsfunksjonene og -innstillingene under leveres klare til bruk på alle (multifunksjons)skrivere fra Sharp, og kan gi en hurtig løsning. Samtlige av dem kan raskt aktiveres/deaktiveres eller justeres av IT-administratoren for å endre standard sikkerhetsnivå og gi en langt mer effektiv beskyttelse ut fra bedriftens konkrete behov:

- Eksempler på lokale administrasjonsinnstillinger: endring av administratorpassord, tilgang til enhetsnettsiden, sikkerhet ved ekstern bruk
- Standardkonfigurasjon av sikkerhetsfunksjoner: portkontroller, protokollinnstillinger, SNMP MIB-innstilling, tilgangsfiltre, SSL, S/MIME, IPSEC, IEEE802.1X, aktivering/deaktivering av protokoller for mobilutskrifter, eksterne serviceinnstillinger, offentlig mappe – nettverksadressert server (delt disk), sporings-ID (utskrift av sporingsinformasjon), brukerinnstillinger, aktivering/deaktivering av alternative løsninger for brukersikkerhet, automatisk sletting av lagrede filer, sletting av hele spolekøen ved feil
- Forbedrede sikkerhetsfunksjoner (i standard sikkerhetsmodus): overskriving av HDD-data (tømming av harddisk) etter hver kopi/utskrift/skanning/faks, lagringskryptering, passordbeskyttelse
- I samme gruppe finnes flere avanserte, valgfrie innstillinger. Gjennom disse innstillingene kan IT-administratorer få tilgang til avanserte Sharp-sikkerhetsfunksjoner for organisasjoner som krever et høyest mulig sikkerhetsnivå (f.eks. statlige og militære organer), eller bedrifter som ønsker å maksimere sikkerheten:

    - DSK (Data Security Kit) inneholder følgende: installering av Data Security Kit, forbedringer av datasikkerheten, forbedringer av utskriftssikkerheten, validering av fastvare
    - Avansert DSK (Data Security Kit) inneholder: HCD-PP-sertifisert avansert sikkerhetsmodus (inkluderer Data Security Kit), forbedret lagringskryptering, skjerpede passordkrav og kontroller av fastvaresikkerheten

### Seks enkle trinn

Sett fra et langsiktig perspektiv vil følgende seks trinn gi deg mulighet til å utvikle og innføre ditt eget konsekvente rammeverk for nettverkssikkerhet på en strukturert måte.

1. **Sikker tilgang til nettverket**
   Hver eneste enhet som er koblet til nettverket, er kun så sikker som det mest sårbare punktet i nettverket. For å opprettholde nettverkssikkerheten er det derfor svært viktig å kontrollere bruken av porter og protokoller. Med en fornuftig konfigurasjon kan IT-administratorene forhindre uønskede aktiviteter og potensielle angrep mot infrastrukturen. Du kan sikre kommunikasjonen mellom nettverket og hver enhet på blant annet følgende måter:

    - Begrens tilgangen til spesifikke IP-adresser ved hjelp av IP-filtrering, og bruk i tillegg MAC-filtrering (Media Access Control). Dette er med på å beskytte nettverket ditt og kommunikasjonskanalene dine ved at det kun er mulig å få tilgang gjennom spesifikke IP-adresser eller -områder.

- Deaktiver porter som ikke er i bruk (slik at det kun er portene du trenger, som fungerer). Dette tilfører et ekstra sikkerhetslag og gir deg mer kontroll over nettverket ved å hindre uautorisert tilgang til tilknyttede ressurser.
- Forsikre deg om at IPSec (Internet Protocol Security for sikker og kryptert utveksling av data), TLS (Transport Layer Security for kryptert dataoverføring) og HTTPS (Hypertext Transfer Protocol Secure for sikker nettverkskommunikasjon) er konfigurert til å gi et høyest mulig beskyttelsesnivå.

**2. Sikre enheten (for å beskytte dataene dine)**
Sikkerheten til de lagrede dataene på harddiskstasjonene (HDD) på (multifunksjons)skriverne kan ivaretas på to måter:

- Datakryptering er en prosedyre eller funksjon som krypterer dokumenter ved hjelp av en kompleks 256-biters algoritme.
- Dataoverskriving brukes for å slette data fra HDD-en til en enhet. Alle lagrede data på stasjonen, samt eventuelle elektroniske bilder av utskrevne dokumenter, overskrives da opptil 10 ganger for å sikre at de slettes permanent.

Hvis du ønsker ekstra fred i sjelen, tilbyr Sharp et leasingslutt-/servicealternativ som sikrer at eventuelle gjenværende digitale data på enheten slettes, og at den fysiske HDD-en destrueres.

**3. Sikker brukertilgang (gjennom brukeridentifisering og -autorisasjon)**
Ett av de viktigste trinnene er å innføre brukeradministrasjon og -autorisasjon, slik at du har kontroll over samtlige brukere. Hovedaktivitetene i denne kategorien er følgende:

- Brukeridentifisering er prosessen som administratorene benytter for å sikre at kun registrerte brukere gis tilgang til (multifunksjons)skriverne. Brukerne må identifiseres ved hjelp av enten lokal godkjenning (ut fra den lokale brukerlisten) eller nettverksgodkjenning gjennom godkjenningsserveren.

- Brukerautorisasjon benyttes for å gi kontrollert tilgang til organisasjonens nettverksressurser. Administratorene kan ut fra påloggingsinformasjonen til hver enkelt bruker begrense tilgangen til bestemte personer, begrense tilgangen til enhetsfunksjoner eller blokkere all tilgang. Tilgangen til enheten kan dessuten konfigureres gjennom ID-kort som inneholder personidentifiserbare data.

**4. Skriv ut konfidensiell informasjon på en trygg måte**
Konfidensielle dokumenter bør kun skrives ut gjennom en sikker prosedyre som hindrer uautorisert tilgang og kopiering. Når en utskriftsjobb sendes, blir den vanligvis plassert i enhetens HDD og frigis derfra først når brukeren har lagt inn en tidligere konfigurert PIN-kode. Når dokumentet er skrevet ut, slettes samtlige data automatisk fra HDD.

**5. Kontroller nettverksaktiviteten**
Implementert på riktig måte kan verktøyene for nettverkssikkerhet gi IT-administratorene full kontroll over alle nettverkstilkoblede enheter, direkte fra skrivebordet. De kan dermed styre en hel (multifunksjons)skriverpark samt oppdage, konfigurere og håndtere de fleste potensielle sikkerhetstrusler. Muligheten til å klone enheter gjør livet enklere for administratorene, ettersom endringer i enhetsinnstillingene enkelt kan tas i bruk for hele parken.

**6. Velg riktig partner**
Det finnes mange selskaper som tilbyr profesjonelle tjenester knyttet til utskriftssikkerhet, men kompetansen kan variere betraktelig. Sharp tar nettverkssikkerhet på største alvor og har det som tyngdepunkt ved all ny produktutvikling. Som produsent evalueres utstyret vårt ut fra spesifikke retningslinjer for omfattende sertifisering etter felleskriterier. Våre nettverkstilkoblede multifunksjonsskrivere med integrert alternativ for datasikkerhet har derfor blitt uavhengig evaluert iht. Japans anerkjente evaluerings- og sertifiseringssystem for IT-sikkerhet (JISEC). De er sertifisert å innfri Protection Profile for Hardcopy Devices v1.0 (HCD-PP v1.0)-standarden i felleskriteriene, og dette betyr at vi kan hjelpe kundene å håndtere maksimalt sensitive data.

## Få eksperthjelp

Selv om alt dette kan virke overveldende, er det viktig å huske at du ikke er alene – du kan når som helst få eksperthjelp.

Sharp tilbyr flere løsninger, verktøy og tjenester for å undersøke eventuelle svakheter i nettverket ditt, forberede en optimaliseringsplan og utarbeide mulige løsningsalternativer du kan velge mellom:

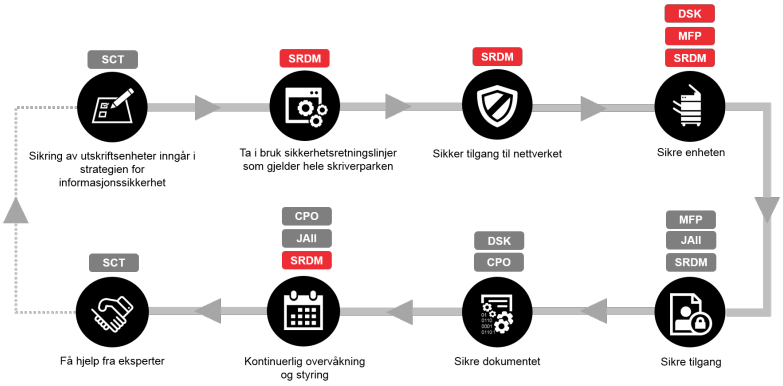
- **Workshop om utskriftssikkerhet**
  Vi har en rekke verktøy og teknologier vi kan bruke for å hjelpe organisasjonen din å få innsikt i sikkerhetstruslene, trekke konklusjoner og utarbeide en skreddersydd optimaliseringsplan.

  I revisjonen vurderes sikkerheten til alle perifere nettverkstilkoblede enheter. I tillegg til de standardmessige og avanserte funksjonene som er tilgjengelige for disse enhetene, kontrollerer vi verktøyene for effektiv registrering og forebygging av trusler. Vi undersøker dessuten om enhetene som brukes i bedriften din, er egnet for formålet og kan gi bedriften og brukerne maksimal sikkerhet. I revisjonen av utskriftssikkerheten skisseres også de videre trinnene for å implementere konsekvente retningslinjer for utskriftssikkerhet og dekke samtlige sikkerhetsaspekter i bedriften. Dette innbefatter følgende:
  - Nettverkssikkerhet – som beskrevet i dette dokumentet
  - Utdatasikkerhet – dette omfatter alle aktiviteter knyttet til dokumentutdata (utskrifter, skanning, faks, sending på e-post)
  - Dokumentsikkerhet – dette går på håndteringen av elektroniske filer og papirfiler som brukes på kontoret
  - Samsvar med personvernforordningen (GDPR) – dette handler om å sikre at de nyeste EU-forskriftene for sikkerhet og personvern innfris.

- **Sikkerhetspakke**
  En kunde-workshop kombineres her med installering av Sharp Remote Device Manager og eventuelt konfigurering og distribuering av systemet for utdatastyring for å omfatte også nettverks- og utdatasikkerhet.

- **Sharp Remote Device Manager (SRDM)**
  Dette Sharp-verktøyet hjelper deg å implementere kritiske sikkerhetsinnstillinger på bare sekunder. Implementeringen blir levert som tjeneste av et profesjonelt Sharp-team. IT-miljøet ditt får relevante sikkerhetsinnstillinger ut fra hva du trenger, og samtlige (multifunksjons)skrivere fra Sharp vil være under kontroll.

**Utarbeidelse av retningslinjer for utskriftssikkerhet samt Sharps løsninger for nettverkssikkerhet**




**SCT** – Sharp Consulting Team, **SRDM** – Sharp Remote Device Manager, **DSK** – Data Security Kit, **MFP** – multifunksjonsskriver, **JAII** – Job Accounting II, **CPO** – Cloud Portal Office

# Konklusjon

## Hva har vi lært! Aldri så galt at det ikke er godt for noe!

Selv om (multifunksjons)skrivere helt klart er en alvorlig (og foreløpig undervurdert) risikofaktor for bedriftene, finnes det konkrete tiltak du kan ta for å beskytte deg.

- **Du er ikke alene – farene lurer overalt.** Hver dag hører vi om brudd på persondatasikkerheten, cyberangrep, virus og annen ondsinnet aktivitet som rammer bedrifter i alle størrelser. Det viktigste er å forstå hvilke konsekvenser det kan få hvis bedriften din skulle bli angrepet, og spørre seg selv: «Er bedriften min virkelig rustet til å forsvare seg?»

- **Løsningen er ikke alltid enkel.** Det kan ta evigheter å fastslå, konfigurere og iverksette egnede sikkerhetstiltak og -funksjoner, og implementeringen kan by på mye hodebry. Ettersom alle organisasjoner er forskjellige, vil det variere hvilke verktøy og strategier du trenger for å gripe an de konkrete truslene som bedriften din står overfor. Uansett hvilke behov du har, kan Sharp imidlertid hjelpe deg å skape en effektiv sikkerhetsløsning for (multifunksjons)skriverne dine.

- **Hvis bedriften din ikke er godt rustet, gjelder det å få klarhet i hva som er problemet.** Hva er det som gjør bedriften din sårbar? Har den verktøyene og ressursene som trengs for å innføre eller skape bedre retningslinjer for nettverks- og utskriftssikkerhet? Eller bør du la spesialister fra Sharp gjøre en revisjon av nettverkene og de nettverkstilkoblede perifere enhetene dine, slik at du kan få anbefalt relevante sikkerhetsverktøy?

- **Sett opp dine egne sikkerhetsmål.** For å få innsikt i potensielle svakheter og hva du trenger å beskytte, må du spørre deg selv følgende: «Hvor vil jeg at organisasjonen min skal være om noen år?» og «Hvordan forbereder jeg bedriften min til å ta trinnene som trengs for å innføre egnede tiltak og

Sikkerhetsrammeverk fra Sharp


verktøy som kan hindre cyberangrep, skadelig programvare osv.?»

- **Sørg for at du har riktig ekspertise.** Hvis du har de nødvendige ressursene på huset, kan du utarbeide dine egne retningslinjer for utskriftssikkerhet. Alternativt kan du la Sharps profesjonelle serviceteam hjelpe deg å bygge et effektivt sikkerhetssystem og innføre verktøy som er relevante for din type virksomhet og behov, herunder:

  - Sikre nettverksenheter fra Sharp som er kompatible med de nyeste sikkerhetssertifikatene
  - Sikkerhetsprogramvare, -løsninger og -tjenester fra Sharp som hjelper deg å få på plass retningslinjer for utskriftssikkerhet: DSK, SRDM, revisjon av utskriftssikkerhet osv.

- **Vi er her for å hjelpe.** Vi kan sørge for at revideringen og implementeringen din av retningslinjer for utskriftssikkerhet går uten unødvendige forsinkelser. Representanter fra Sharp står klar til å hjelpe deg å kartlegge og vurdere ditt nåværende sikkerhetsnivå, samt foreslå en strategi for å få på plass konsekvente retningslinjer for

utskriftssikkerhet tilpasset bedriftens behov og krav. Våre eksperter hjelper deg å plukke ut relevante verktøy og tjenester blant følgende:

- Standard sikkerhetsfunksjoner fra Sharp
- Valgfrie verktøy som f.eks. SRDM
- Valgfrie optimaliseringer som f.eks. DSK
- Nettverkssikkerhetspakke fra Sharp
- Sikkerhetsrevisjon fra Sharp
- Retningslinjer for utskriftssikkerhet

- **Se ting i et større perspektiv.** For at du skal unngå potensielle svakheter på andre områder i organisasjonen din, kan vi hjelpe deg å innføre ytterligere sikkerhetstiltak fra Sharp-porteføljen. På den måten kan du sørge for at hvert eneste aspekt av virksomheten beskyttes fullt ut:
  - Nettverkssikkerhet
  - Utdatasikkerhet
  - Dokumentsikkerhet
  - Samsvar med personvernforordningen

Du finner mer informasjon om alle sikkerhetsløsningene våre i «white paper» biblioteket og under delen om informasjonssikkerhet på nettstedet vårt: https://www.sharp.no/cps/rde/xchg/no/hs.xsl/-/html/informasjonssikkerhet.htm

Alternativt kan du kontakte en løsningskonsulent fra Sharp.

# Referanser


1. «Eastern and Western Europe Single-Function Printer & MFP Market Placements in the last five years», rapport fra IDC, 4. kvartal 2018
2. «IT and Print Security Survey 2015», IDC, september 2015
3. «Printing: a false sense of security», Quocirca, 2013
4. «Transformative Technology in Document Security», IDC, mai 2015

www.sharp.no

SHARP

Be Original.