

# Dokumentsäkerhet

Skydda affärsinformationen

# Innehåll

<b>Introduktion</b> .....	3
<b>Bakgrund</b> .....	4
<b>Problem</b> .....	5
<b>Rekommendationer</b> .....	7
<b>Slutsats</b> .....	10
<b>Referenser</b> .....	11

# Introduktion

Varje dag behandlar organisationer tusentals dokument i alla möjliga format, och varje dag riskerar dokument att tappas bort, stjälas eller manipuleras. De behöver skyddas.

Sharp definierar dokumentssäkerhet som säkerhet relaterad till information som scannats från pappersdokument, eller digitala dokument som lagras i datalager, exempelvis Microsoft Office-filer och e-postmeddelanden. Sharps lösning för dokumentssäkerhet omfattar:

- Dokumentrelaterade affärsprocesser
- Dokumentlagring (pappersdokument och digitala filer)
- Dokumentlivscykel (Scanning → Lagring → Hantering → Arkivering → Överlämning → Integration)

I det här faktabladet beskrivs de utmaningar varje företag ställs inför när det gäller dokumentssäkerhet. Huvudsakliga punkter som beskrivs:

- **Bakgrund**

Analys av komplexiteten hos dokumentssäkerhet. Behandlar allt från identifiering av kontorsdokument och information för de vanligaste affärsprocesserna till särskiljande mellan pappersbaserade dokument och digitala filer och en beskrivning av dokumentets livscykel.

- **Problem**

En beskrivning av de utmaningar som IT-chefer, användare och företagsledning kan möta utifrån ett dokumentssäkerhetsperspektiv, speciellt vid scanning, lagring och åtkomst av affärskritiska dokument och annan känslig information. Fokusområdena är:

- Ostrukturerade data
- Manuella uppgifter relaterade till kontorsdokument
- Övergripande dokumentssäkerhet

- **Rekommendationer**

Beskrivning av hur Sharps optimerade lösningar, tjänster och rutiner kan bidra till att skapa en säker dokumentmiljö som skydd mot dokumentrelaterade hot som kan leda till incidenter eller processtörningar. I det här avsnittet beskrivs även hur Sharp kan hjälpa till att lösa komplexa affärsproblem inom följande områden:

- Dokumentprocessers betydelse och roll
- Optimering av pappersbaserade arkiv och datalager med digitala filer
- Identifiera alla steg som krävs för att optimera dokumentets livscykel och skapa en egen policy för dokumentssäkerhet och effektiva rutiner.

- **Slutsats**

En sammanfattning av ämnet med fokus på:

- Företagets största utmaningar relaterade till verksamhetens dokument
- Huvudsakliga rekommendationer baserade på Sharps expertis och optimerade lösningar
- Nästa steg som erfordras för att skapa en enhetlig policy för dokumentssäkerhet
- Knyta samman dokumentssäkerhet med andra säkerhetsaspekter såsom nätverkssäkerhet och utskriftssäkerhet

# Bakgrund

## Arbetstakt och datavolymer ökar exponentiellt på dagens arbetsplatser.

Enligt marknadsanalysinstitutet IDC förväntas den globala produktionen av data öka till hela 163 zettabyte (ZB) år 2025<sup>1</sup>. Det är 10 gånger så stor volym jämfört med år 2017.

Varje dag framställs avtal, fakturor, offerter och många andra dokument i många olika format, vilka alla är viktiga i företagets verksamhet.

Via avtal definieras exempelvis den affärsmässiga relationen mellan ett företag och dess kunder, medan fakturor är nödvändiga för verksamhetens intäkter. Det är helt nödvändigt för ett företags funktion att hantera, arkivera och göra denna information tillgänglig för rätt personer inom företaget.

*90 % av alla nuvarande data har skapats under de senaste två åren; det motsvarar 2,5 triljoner byte data per dag.<sup>2</sup>*

Volymen, komplexiteten och mångfalden av den information som ett företag framställer och använder medför utmaningar avseende både hantering och övervakning. Om företaget ska lyckas bemästra dessa utmaningar krävs förståelse och kartläggning av de olika dokumenttyperna; hur de används, interagerar med affärsprocesser, lagras, hanteras, distribueras och arkiveras.

De flesta utmaningarna är direkt kopplade till följande tre områden:

- **Ostrukturerade data**

Ostrukturerade data är information utan någon fördefinierad datamodell eller som inte är strukturerad på ett fördefinierat sätt. Ofta lagras användarna transaktionsdokument såsom e-post eller andra dokument i mappstrukturer utan någon standardiserad namngivningskonvention eller beskrivande metadata.

Det är av denna anledning mycket svårt att få någon överblick vilket gör det svårt att besvara följande frågor:

- Hur lagras, hanteras och övervakas dokument?
- Kan dokument enkelt hittas, spåras och distribueras?
- Hur tillämpas behörighetsnivåer och filrättigheter?

- **Manuella, återkommande uppgifter**

Manuella, återkommande uppgifter förekommer i praktiskt taget alla verksamheter, oavsett om det handlar om fakturor eller hantering av kostnader eller personalrelaterade dokument. Tekniken kan hjälpa till att automatisera dessa processer, vilket ger högre effektivitet, bättre noggrannhet, bättre spårbarhet och ökad säkerhet.

- **Klargörande av dokumentets hela livscykel**

Varje dokument eller dokumenttyp har en livscykel från scanning till permanent radering. Det är väsentligt att förstå, kartlägga och optimera dokumentets livscykel för olika dokumenttyper för att säkerställa att företaget tillämpar effektiva säkerhetsåtgärder och därmed efterlever gällande regelverk. Genom detta uppnår man även den flexibilitet som krävs för att arbetsrutinerna ska löpa så effektivt som möjligt.

Detta är nyckelområden som varje företag bör tänka på när man definierar och inför en policy för dokumentssäkerhet i organisationen.

# Problem

Dagens företag behandlar en mängd information, men har ofta inte någon verklig inblick i hur den produceras, lagras och nås, vilket leder till potentiella säkerhetsbrister.

De flesta organisationer skapar och lagrar digitalt innehåll; dokumenten lagras emellertid ofta i två format – digitalt och i pappersform.

- **Pappersdokument**

Pappersbaserade dokument utgör en stor säkerhetsrisk, eftersom det ofta är svårt att redovisa dokumentens ursprung eller spårningsinformation. Dessutom förbises ofta den fysiska säkerheten, då känsliga dokument exempelvis kan komma bort eller arkiveras på fel plats eller på osäkra platser.

- **Digitala filer**

Digitala filer lagrade i spridda och ibland isolerade lagringssystem utgör en säkerhetsutmaning i sig självt på grund av de ofta stora volymerna och mångfalden av lagringssystem eller lagringsmiljöer. Kunskap om dokumentens livscykel är det enda sättet att fastställa rutiner och säkerhetspolicy på alla nivåer i företaget.

## Upprätthålla hög dokumentssäkerhet

Definitionen av dokumentssäkerhet (eller brist på) är mycket bred och bör utgå från ett perspektiv som omfattar hela dokumentlivscykeln, speciellt i relation till incidenter, ostrukturerad data, oskyddade filer, mänskliga misstag, obehörig åtkomst till datalager etc.

Dokumentlivscykeln omfattar sex faser: Scanning – Lagring – Hantering – Arkivering – Överlämning – Integration

- **Fas 1: Scanning**

Scanning är den processfas som omfattar informationens "födelse", oavsett om den utgörs av scanning av pappersdokument, övervakning av en epostadress eller att skapa och spara dokument från en mjukvara.

- **Scanning** är det vanligaste sättet att omvandla innehållet i pappersdokument

till digitala format. Scanning är en praktisk metod, men kan emellertid leda till problem avseende säkerhet eller juridiskt värde. Utan kontroll är processen inte spårbar, vilket innebär att dokument riskerar att sakna bevisvärde och juridiskt värde.

- **Indexering** är en metod som används för att beskriva dokument med hjälp av metataggar eller fritext. Indexering underlättar snabb fil- och datasökning, och är speciellt användbar för granskning av innehåll avseende efterlevnad av säkerhet.
- **Dirigering** innebär att scannade dokument skickas till en viss lagringsdestination. Utan dokumentdirigering föreligger risk att dokument oavsiktligt lagras på felaktiga eller till och med osäkra platser.

- **Fas 2: Lagring**

Säker lagring kan vara pappersbaserad eller ett system för digitala filer. Många företag förbiser emellertid kraven på lagringstyp, lagringsplats och säkerhet:

- Pappersbaserade lagringssystem är fortfarande mycket vanliga, men saknar ofta nödvändiga säkerhetsfunktioner. Det är dessutom mycket svårt att redovisa någon spårningsinformation för pappersdokument
- Digitalt baserad lagring förutsätts ofta vara ett bättre sätt att lagra dokument. Om ett sådant system inte utarbetas och administreras korrekt kan emellertid svårigheter uppstå, bland annat avseende hur systemet ska skyddas i företagsnätverket, hur behörigheter ska tilldelas och hur användning ska övervakas eller begränsas.

- **Fas 3: Hantering**

Dokumenthantering omfattar behörigheter, versionskontroll och spårningsinformation:

- Behörigheter används för att hantera användarnas åtkomsträttigheter till dokument, och är därför avgörande för en säker dokumentmiljö. Även om behörigheter ofta är enkla att förstå kan de vara svåra att införa och hantera utan rätt system. För effektiv implementering av behörigheter är det viktigt att först förstå hur användarnas aktiviteter är relaterade till informationen de behöver ha tillgång till och de rutiner de är involverade i.
- Versionskontroll säkerställer att användarna arbetar med den senaste dokumentversionen, samtidigt som tidigare versioner vid behov kan arkiveras. Detta är särskilt användbart i strategiska eller rättsliga sammanhang där dokumentets ursprung kan bevisas genom granskning av tidigare dokumentgenerationer. Versionskontroll är avgörande för ett säkert digitalt dokumentarkiv av juridiskt värde.
- Spårningsinformation avser information om alla aktiviteter och transaktioner för ett dokument, bland annat vem som har skapat, modifierat, visat eller ändrat version för dokumentet. Den gör det också möjligt att redovisa alla aktiviteter avseende alla lagrade dokument, vilket är avgörande för en hög säkerhetsnivå, i synnerhet i händelse av incidenter.

- **Fas 4: Arkivering**

Arkivering av dokument och information är ytterligare en viktig aspekt för en säker dokumentmiljö. För dokument lagrade i traditionella eller digitala arkiv krävs emellertid fortlöpande underhåll eftersom tillgängligt utrymme är begränsat. Följande rutiner är därmed centrala:

- **Dokumentarkivering**

Vissa dokument måste enligt lag arkiveras ett visst antal år. Utmaningarna relaterade till detta krav är:

- Säkerställa att endast dokument som är äldre än lagstadgad arkiveringstid tas bort vid underhållsarbete

- Säkerställa att alla versioner av ett dokument sparas under lagstadgad arkiveringstid
- Fastställa hur dokument ska hanteras centralt eller lokalt

- **Dokumentradering.**

Företagen måste införa en policy som säkerställer säker radering av all pappersinformation och digitala filer och bibliotek när de blir förlegade eller arkiveringstiden har löpt ut:

- Fysisk dokumentförstöring enligt någon av DIN Shredding Security-standarderna är det traditionella sättet att kassera pappersdokument. Det blir emellertid lätt en kostsam och tidskrävande process.
- Digital rensning innebär säker och verifierbar radering av digital information på hårddiskar, dvd-skivor, disketter etc

- **Fas 5: Överlämning**

Denna fas definierar hur digitala dokument kan delas med andra användare eller affärspartner. De viktigaste aspekterna är:

- Dokumentdelning görs ofta genom användning av delade mappar eller enheter. Om detta inte hanteras på rätt sätt riskeras emellertid att filer blir åtkomliga för obehöriga användare.
- Överlämningsfasen kan även omfatta åtkomst av dokument via mobila enheter, vilket gör problemet med säker åtkomst ännu mer komplext.

- **Fas 6: Integration**

Integrering innebär utbyte av information med tillämpningar inom andra affärsområden, exempelvis redovisnings- eller ERP-system.

Om integrationen ska lyckas är det avgörande att alla tidigare faser har utförts korrekt och fullständigt för att säkerställa överensstämmande och korrekta data. Om problem föreligger i någon av de tidigare faserna får detta en direkt inverkan på affärsprocessen.

# Rekommendationer

Sharp kan erbjuda flera olika lösningar och tillämpningar som kan underlätta för organisationen att skapa en erforderlig policy för datasäkerhet.

Dokumentsäkerhet är ett mycket komplext ämne, men genom att definiera strukturen för dokumentets livscykel kan man lättare få en överblick över problemet och därefter göra nödvändiga ändringar eller förbättringar:

- Det kan vara mycket svårt och tidskrävande att förbättra processer eller definiera dokumentsäkerhet från grunden, speciellt när det gäller att kartlägga processer och sammanställa all relevant information om processer och affärsområden. Sharp Professional Services drar nytta av både Sharps erfarenhet av dokumentlösningar och avancerade verktyg för att sammanställa dokument och information samt kartlägga arbetsflöden.
- Sharp utnyttjar en stegvis process som gör att företaget lättare får överblick över sin nuvarande dokumentlivscykel och relaterade utmaningar. Utifrån detta utarbetas därefter processer och rutiner som är kopplade till de två huvudsakliga målen för optimering av dokumentsäkerheten:
  - Skapa en struktur för ostrukturerade data
  - Snabba upp och effektivisera återkommande uppgifter

## Snabb och säker igångsättning

- Sharp kan hjälpa kunden att skapa en robust säkerhetspolicy och dokumentmiljö. Vår kombination av Sharp multifunktionssystem för scanning och optimerade mjukvarulösningar för lagring och hantering av dokument är en lösning som ger kunden trygghet samt en säker och spårbar dokumentinfrastruktur.
- Det kan vara lämpligt att börja göra processförändringar för dokumentintensiva avdelningar (personal-, ekonomi-,

juridikavdelningen etc), och så småningom stegvis utvidga processer och rutiner till andra områden av verksamheten.

## Förenkla scanning och lagring av dokument

- För att säkerställa säker scanning rekommenderar Sharp starkt att scanningfiler lagras enbart i säkra, interna datalager och hos utvalda användare eller användargrupper som alla kan konfigureras av IT-administratören. Detta är speciellt viktigt med tanke på efterlevnad av den allmänna dataskyddsförordningen.
- Vid krav på mer avancerade funktioner, exempelvis av juridiska skäl, finns Sharps optimerade mjukvarulösningar att tillgå. Sharp erbjuder en rad olika lösningar som påskyndar processer i små, medelstora och stora organisationer, och som möjliggör direkt integration med affärstillämpningar.
- Med Sharps optimerade lösningar kan alla scannade dokument indexeras:
  - Lägg till metadata direkt från multifunktionssystemet
  - Lägg till metadata i tillämpningen innan dokumentet lagras och behandlas vidare
- Sharps optimerade lösningar inkluderar funktioner för dirigering som säkerställer att alla användare kan scanna dokument på samma, strukturerade sätt och därefter dirigera dokumenten till korrekt plats och tillförlitliga tillämpningar.

## Användarroller och behörigheter

När en policy för dokumentsäkerhet utarbetas är användarbehörigheter och roller viktiga för att konfidentialitet och övervakning ska säkerställas.

- Sharp rekommenderar att ett centralt dokumenthanteringssystem med "roller" kopplade till personalens arbetsuppgifter och behov används. Till exempel:

- Endast företagsledningen ska ha tillgång till alla affärsdokument
- Endast personalavdelningen ska ha tillgång till all personalinformation
- Projektchefer ska ha tillgång till projektrelaterade dokument
- Säljare ska ha tillgång till säljrelaterat material såsom broschyrer, formulär etc

- Behörigheter definieras baserat på roll eller användargrupp, och bestämmer vad användaren kan göra med dokument – skapa, visa, ändra, radera – eller enbart en viss åtgärd såsom att visa dokument utan några andra rättigheter.
- Versionskontroll är nödvändigt. Med Sharps optimerade lösningar kan du kontrollera vilken version av dokumentet du arbetar med, och granska eller återställa äldre versioner av dokumentet.
- Parallellt arbete med ett dokument är möjligt; medan en användare redigerar ett dokument har övriga användare endast läsrättigheter.
- Efterlevnad av säkerheten kan säkerställas via ett avancerat administrationsverktyg för spåringsinformation (loggning) som registrerar alla dokumentaktiviteter, såsom när ett dokument har ändrats, vem som ändrade det och hur lång tid användaren arbetade med dokumentet.

### Behåll specifik information under en specifik tidsperiod

- Utarbeta en policy för dokumentarkivering baserat på dokumenttyp och de avdelningar som behandlar informationen.
- Dokumentradering är slutpunkten för policyn för dokumentarkivering. Beroende på vilken typ av dokumentlager som används kan en mängd data tas bort i ett svep från systemet:
  - För pappersdokument rekommenderas en professionell dokumentförstörare klassad enligt DIN 5 eller högre
  - För digitala data rekommenderas en professionell utrustning eller mjukvara för permanent dataradering

- För data lagrad på hårddiskar (via dokumenthanteringsprogram och interna dokumentlager) rekommenderas en process i två steg: datarensning följt av fysisk destruktions av hårddisken som omöjliggör åtkomst av data.

### Transparent åtkomst och delning av information

En policy för dokumentsäkerhet ska alltid inkludera en beskrivning av hur användarna kan få tillgång till dokument och dela information med andra.

Sharps optimerade lösningar erbjuder flera olika metoder för delning av dokument via dokumenthanteringsplattformen:

- En möjlighet är att dela en tidsbegränsad länk till filen via e-post till en eller flera adressater. Alla detaljer om delningen loggas, och länken kan avslutas på begäran eller via en förinställd tidsgräns.
- Ett annat alternativ är att dela mappar i systemet med registrerade användare i samma organisation. Du kan bestämma och konfigurera vilka rättigheter – läsrättigheter, läs- och skriv-rättigheter eller läs-, skriv- och raderingsrättigheter – mottagaren ska ha vid arbete med dokumenten i mappen. Dessa rättigheter och regler kan även fastställas vid utformning av de övergripande reglerna för dokumenthanteringssystemet och policyn för dokumentsäkerhet.
- De flesta av systemets funktioner kan göras tillgängliga även för mobila användare som använder exempelvis Android- eller iOS-plattform. Sharp rekommenderar att varje företag beaktar fördelarna med säkert mobilt arbete.

### Optimalt värde av företagets data

Sharp har utvecklat ett antal integrationer vilket betyder att data scannade via ett Sharp multifunktionssystem, bevakade mappar eller ansluten mjukvara, kan integreras med affärssystem såsom Sage, QuickBooks, SharePoint etc.

Exempel på avdelningar som Sharp har fokuserat på:



- **Optimised Workflow Software för digital hantering av inkommande fakturor**

Lösningen använder optisk teckenigenkänning (OCR) för att extrahera data från scannade fakturor, och automatiserar validerings- och godkännandeprocesserna.

Ekonomiavdelningen får därmed högre produktivitet, bättre noggrannhet och högre effektivitet.

- **Optimised Workflow Software för digital posthantering**

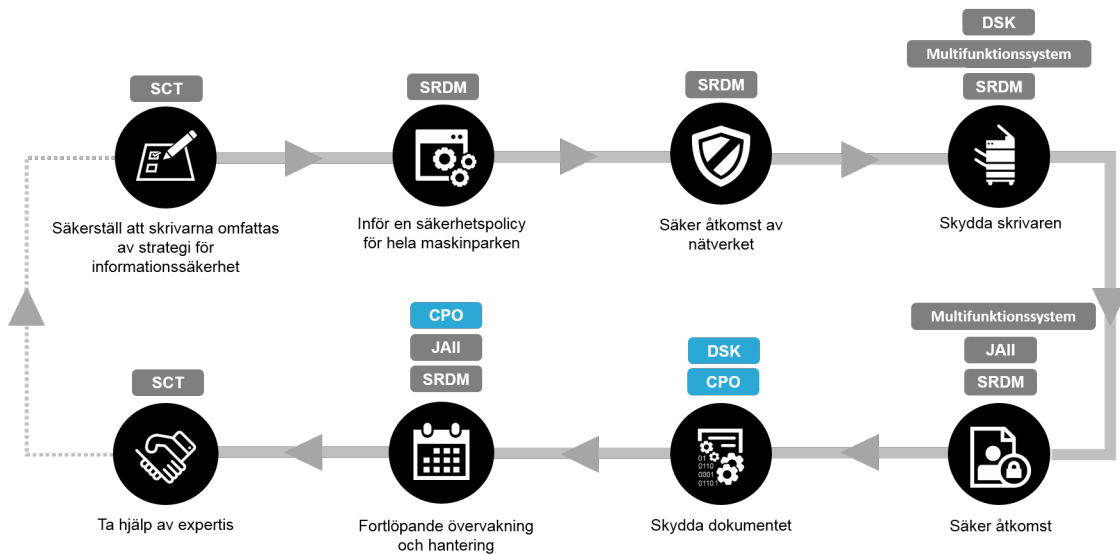
Denna lösning skannar inkommande pappersbaserad och digital post och dirigerar den digitalt till rätt användare om denne inte befinner sig på kontoret. Stora postvolymen kan på så sätt snabbt och effektivt sorteras

och distribueras, vilket gör att personalens produktivitet maximeras.

- **Optimised Workflow Software för personalavdelningen (HR)**

Denna lösning innefattar ett mycket säkert och övervakat dokumentlager för konfidentiell personaldokumentation. Företag kan därmed effektivisera behandlingen av HR-dokument, tilldela behörighet till dokument och säkerställa efterlevnad av den allmänna dataskyddsförordningen.

### Utarbeta en policy för utskriftssäkerhet och en Sharp-lösning för dokumentsäkerhet



SCT – Sharp Consulting Team, SRDM – Sharp Remote Device Manager, DSK – Datasäkerhet, Multifunktionssystem, JAII – Job Accounting II, CPO – Cloud Portal Office

# Slutsats

Ingen har råd att ignorera informationssäkerhet, speciellt när det handlar om dokument. De är varje organisations intellektuella kapital, och en förlust av dessa kan vara förödande.

Dokumentsäkerhet är en av de viktigaste säkerhetsaspekterna i alla företag. Att utarbeta en policy för dokumentsäkerhet kan emellertid vara en tidskrävande och komplex process. Här kan Sharp vara till stor hjälp.

Sharp har tack vare mångårig erfarenhet av dokumentlösningar kunnat utveckla en totallösning för datasäkerhet i företag; från nätverkssäkerhet och utskriftssäkerhet till dokumentsäkerhet.

Vi strävar efter att hjälpa våra kunder att utarbeta robust och regelrätt säkerhet avseende dokumentrelaterade affärsprocesser med hjälp av vår expertis och globalt erkända ledarskap inom säkerhet.

Med hjälp av vår beprövade metod för dokumentsäkerhet hjälper vi företag att skapa unika och skraddarsydda system och processer för varje steg i dokumentets livscykel (scanning, lagring, hantering, arkivering, överlämning och integration), och därmed efterleva alla gällande regelverk inklusive den allmänna dataskyddsförordningen.

Sharps optimerade lösningar är utvecklade för maximal funktionalitet och säkerhet, tillsammans med en snabb avkastning på investeringen.

Några av Sharps viktigaste områden är myndigheter, utbildning, juridik, finans, hälso- och sjukvård, hotell- och restaurangbranschen och storföretag. Vi kan emellertid leverera skraddarsydda, robusta lösningar för alla verksamhetstyper.

För att undvika potentiella risker inom andra områden av din organisation kan vi hjälpa till att

## Sharp Security Framework



höja den generella säkerhetsnivån med verktyg och tjänster från Sharps portfölj:

- Dokumentsäkerhet
- Nätverkssäkerhet
- Utskriftssäkerhet
- Efterlevnad av den allmänna dataskyddsförordningen

Mer information om ovanstående ämnen finns i vårt faktabladsbibliotek och även på sidorna med informationssäkerhet på vår webbplats: <https://www.sharp.se/cps/rde/xchg/se/hs.xsl/-/html/skydda-din-information.htm>

Du kan även kontakta din lokala Sharp återförsäljare.

# Referenser

1. "Data Age 2025", IDC, mars 2017
2. "Data Never Sleeps 5.0", DOMO, 2018

