

Faktaägare Regionarkivarie
Gäller för: Alla

INSTRUKTION

Datum 2020-12-18
Version 1.0

1 (9)

Krav på systemstöd för hantering och förvaring av digitala dokument

Innehåll	
Inledning	3
Ansvar	3
Syfte	3
Avgränsning	3
Målgrupp.....	3
Krav på systemstöd	3
Arbetsflöden	3
Behörighetsstyrning	3
Digital signatur	4
Filformat.....	4
Gallring.....	4
Metadata.....	4
Tillgänglighet.....	4
Versionshantering	5
Flyttbara lagringsenheter	5
Molntjänster.....	5
Kravuppfyllnad av systemstöd och lagringsytor för digitala dokument	6

Inledning

Information i Region Skåne ska vara tillgänglig, riktig och sökbar. Det ska gå att lita på att informationen är korrekt och att den alltid är tillgänglig för behöriga. Informationshanteringen ska vidare präglas av öppenhet och möjliggöra allmänhetens rätt till insyn i Region Skånes verksamheter. Mycket av den information som hanteras i Region Skåne ska dessutom bevaras för framtiden. Informationen ska hanteras och förvaras i systemstöd med funktionalitet som möjliggör efterlevnad av kraven.

Ansvar

Alla medarbetare har ett ansvar för att dokument som inkommer eller upprättas förvaras och hanteras i enlighet med nedan listade krav liksom för att de hålls ordnade så att de lätt går att hitta.

Syfte

Syftet med denna instruktion är att ge en samlad kravbild för vad som gäller för att hantera och förvara digitala dokument i Region Skåne samt att fungera som vägledning vid val av systemstöd.

Avgränsning

Gäller inte information som omfattas av patientdatalag (2008:355) då det bland annat ställs andra krav på uppföljning av och åtkomst till personuppgifter inom hälso- och sjukvård.

Gäller inte information som är säkerhetsskyddsklassificerad och som omfattas av säkerhetsskyddslagen (2018:585).

Målgrupp

Instruktionen riktar sig till medarbetare inom Region Skåne som hanterar dokument och behöver vägledning i val av systemstöd.

Krav på systemstöd

Följande krav ska systemstöd uppfylla för att möjliggöra regelefterlevnad och en effektiv och kontrollerad hantering av digitala dokument.

Arbetsflöden

För att säkerställa riktigheten av i första hand styrande dokument ska det finnas arbetsflöden för granskning och godkännande. Vem som granskat och godkänt dokumenten och när det är gjort ska dokumenteras.

Behörighetsstyrning

Behörighetstilldelning görs i huvudsak utifrån funktion, arbetsuppgifter och arbetsområde. Behörighet ska styras till vad man kan och får göra i systemet. Till exempel läsa, skriva, ändra och signera.

Dokument som innehåller sekretessbelagda uppgifter, känsliga personuppgifter eller uppgifter som bedöms integritetskänsliga och skyddsvärda kräver särskild behörighet och åtkomst. Det ska finnas dokumenterade rutiner för ändring, borttagning och regelbunden uppföljning av behörigheter för att säkerställa att dessa är riktiga och aktuella. Varje användares identitet ska kunna verifieras och alltid vara spårbar till en fysisk person.

Digital signatur

Signering av dokument ska ske digitalt med undantag för dokument som enligt lag ska var egenhändigt underskrivna. Dokument som signeras manuellt för att sedan skannas in uppfyller inte kraven i lagen om tillgänglighet till digital offentlig service (2018:1937).

Filformat

Information som förvaras digitalt ska uppfylla krav som främjar långtidsbevarande och behöver därför kunna sparas i eller konverteras till arkivbeständiga filformat:

- Fotografi: TIFF eller JPEG
- Illustration: TIFF eller JPEG
- Karta: TIFF
- Ljud: MP3, PCM eller PCM baserad Wave
- Text: TIFF, XML (utf-8), PDF/A-1a eller PDF/A-1b
- Video: MPEG2 eller MPEG4

Gallring

Dokument ska löpande rensas eller gallras enligt fastställda regelverk¹ för att underlätta sökbarhet samt undvika höga lagringskostnader och resurskrävande merarbete vid systemavveckling. Särskilda krav på gallring ställs på dokument som innehåller känsliga personuppgifter i enlighet med Dataskyddsförordningen.

Metadata

Obligatoriska metadata i systemstöd för dokumenthantering finns beskrivet i RD-beslutet *Baskrav för dokumenthantering i Region Skåne, dnr:1400182*.

Genom att tagga dokument med metadata kan informationen återsökas, tolkas och placeras i ett sammanhang. Metadata säkerställer informationens äkthet, tillförlitlighet och riktighet. Utifrån angiven metadata går det även att bedöma om informationen ska bevaras eller gallras.

Tillgänglighet

Behörig användare ska ha tillgång till den information som behövs för att utföra sina arbetsuppgifter. Informationen ska hållas ordnad och sökbar för att kunna lämnas ut vid begäran om utlämnande av allmän handling.²

¹ Se gällande centrala regelverk under rubriken Arkiv- och informationshantering på vardgivare.skane.se alternativt lokalt framtagna dokumenthanteringsplaner.

² Se vidare i instruktionen *Hantering av handlingar - registrering, posthantering och utlämnande*, Region Skåne.

Versionshantering

Region Skånes medarbetare ska kunna lita på att informationen i dokumenten är korrekt. Ändringar i både metadata och innehåll ska kunna följas upp i dokumenterade loggar och äldre versioner ska kunna återskapas. För detta krävs funktioner för versionshantering.

Flyttbara lagringsenheter

Flyttbara lagringsenheter som externa hårddiskar och USB-minnen ska undvikas eftersom den sortens enheter snabbt blir föråldrade och informationen riskerar att bli oläsbar. Det är även lätt hänt att flyttbara lagringsenheter kommer bort, värdefull information går förlorad eller känsliga uppgifter kommer i orätta händer. Om känslig eller värdefull information trots det behöver lagras på USB-minne ska krypterat USB-minne användas.

Molntjänster

För offentliga myndigheter är rättsläget oklart när det gäller användning av molntjänster. Information som kan omfattas av sekretess eller som innehåller känsliga personuppgifter ska och får inte hanteras i molntjänster som OneDrive och SharePoint online som ingår i Office 365.

Risker och konsekvenser ska noga övervägas innan molntjänster används i Region Skåne, oavsett vilken information som ska hanteras i tjänsten. Beslut om att hantera information i en molntjänst ska fattas av informationsägaren³ och ska alltid föregås av informationsklassificering och riskanalys i enlighet med Region Skånes instruktioner⁴. Beslutet ska signeras och diarieföras.

³ Beslut om informationsägare, RD-beslut 2018-05-22 Dnr: 1800025

⁴ Instruktion för riskhantering avseende informationstillgångar, RD-beslut 2018-10-15 Dnr: 1800025

INSTRUKTION

Faktaägare Regionarkivarie
Gäller för: Alla

Datum 2020-12-18
Version 1.0

6 (9)

Kravuppfyllnad av systemstöd och lagringsytor för digitala dokument

Tabell 1 Kravuppfyllnad av systemstöd och lagringsytor för dokumenthantering

Namn	Definition och alternativa namn	Förvaltning	Arbetsflöden för granskning och godkännande	Digital signatur	Funktioner för automatisk eller halvautomatisk gallring	Lämplig för hantering av sekretess och känsliga personuppgifter	Uppfyller baskrav på metadata	Kommentar och exempel på information som kan hanteras
DokIT	OpenText ContentServer Lagring sker på intern server.	Region Skåne	Ja	Ja	Ja	Ja	Ja	Kan hantera samtliga dokumentslag. Även lämplig för känsliga personuppgifter och information som kan omfattas av sekretess, men inte för information som omfattas av patientdatalagen (2008:355), ändamål vård och behandling.
Dokument-portalen	Läsportalen Författarportalen SharePoint 2016 On-Premise Lagring sker på intern server.	Främst vård-förvaltningarna	Ja	Nej, men har en signatur som bekräftar att man tagit del av innehåll	Nej	Nej	Ja	Kan hantera samtliga dokumentslag med undantag för information som kan omfattas av sekretess eller innehåller känsliga personuppgifter då behörighetsstyrning inte är anpassad för detta. Avsedd och anpassad för i första hand styrande dokument inom vården.
Flyttbara lagringsenheter	USB, extern hårddisk		Nej	Nej	Nej	Nej	Nej	Används för att tillfälligt flytta filer, ingenting ska lagras här under längre tid. Se till att rensa efter hand. Använd krypterade USB-minne vid hantering av information som kan omfattas av sekretess eller innehåller känsliga personuppgifter.
Gemensamma kataloger	I: G: K: osv. Lagring sker på Intern server.	Region Skåne	Nej	Nej	Nej	Nej	Nej	Kan användas för hantering av arbetsmaterial i form av exempelvis utkast och underlag. Ytan får inte användas för information som kan omfattas av sekretess eller innehåller känsliga personuppgifter då det saknas tillräckliga rutiner för tilldelning och uppföljning av behörigheter.

Namn	Definition och alternativa namn	Förvaltning	Arbetsflöden för granskning och godkännande	Digital signatur	Funktioner för automatisk eller halvautomatisk gallring	Lämplig för hantering av sekretess och känsliga personuppgifter	Uppfyller baskrav på metadata	Kommentar och exempel på information som kan hanteras
Hedda	Regionservice lednings- och dokumenthanteringssystem, SharePoint 2016 On-Premise Lagring sker på intern server.	Region-service	Ja	Nej	Nej	Nej	Ja	Används för redovisande och styrande dokument. Ytan får inte användas för information som kan omfattas av sekretess eller innehåller känsliga personuppgifter då dokument lagras i molntjänst i 28 dagar pga. arbetsflöden.
Hemkatalog (Personlig)	H: Lagring sker på intern server.	Region Skåne	Nej	Nej	Nej	Se kommentar	Nej	Kan användas för hantering av arbetsmaterial i form av exempelvis utkast och underlag. Kan endast användas för att tillfälligt hantera en mindre mängd uppgifter som omfattas av sekretess dock inga patientuppgifter eller information som omfattas av absolut sekretess ex vid upphandling.
Kunskapsbanken	ACE Knowledge, Telia Lagring sker i molntjänst.	Region-service, Skåne- trafiken	Ja	Nej	Nej	Nej	Ja	Används av supportfunktioner. Ytan får inte användas för information som kan omfattas av sekretess eller innehåller känsliga personuppgifter då behörighetsstyrning inte är anpassad för detta och lagring sker i molntjänst.
Långa listan	Dokumentportal SharePoint 2016 On-Premise Lagring sker på intern server.	Medicinsk Service	Nej	Nej	Nej	Nej	Ja	Används för redovisande och styrande dokument. Ytan får inte användas för information som kan omfattas av sekretess eller innehåller känsliga personuppgifter då behörighetsstyrning inte är anpassad för detta.
Omnia	SharePoint 2016 Online Lagring sker i molntjänst.	Skåne- trafiken	Ja	Nej	Ja	Nej	Ja	Kan hantera samtliga dokumentslag. Ytan får inte användas för information som kan omfattas av sekretess eller innehåller känsliga personuppgifter då lagring sker i molntjänst.
OneDrive	Office 365, OneDrive för företag, OneNote Lagring sker i molntjänst.	Region Skåne	Nej	Nej	Nej	Nej	Nej	Avsedd för medarbetarens egna dokument. Ytan får inte användas för information som kan omfattas av sekretess eller innehåller känsliga personuppgifter då behörighetsstyrning inte är anpassad för detta och lagring sker i molntjänst.

Namn	Definition och alternativa namn	Förvaltning	Arbetsflöden för granskning och godkännande	Digital signatur	Funktioner för automatisk eller halvautomatisk gallring	Lämplig för hantering av sekretess och känsliga personuppgifter	Uppfyller baskrav på metadata	Kommentar och exempel på information som kan hanteras
Outlook	Microsoft Outlook, RS-mail, Microsoft Exchange, Office 365 Lagring sker i molntjänst.	Region Skåne	Nej	Nej	Nej	Nej	Nej	E-post som behövs för bevakning och pågående arbete. Outlook ska inte användas för långtidslagring utan rensas löpande. Känsliga personuppgifter eller information som omfattas av sekretess ska skickas med säker e-post och ska inte lagras i e-post-systemet längre än nödvändigt. Informationen ska överföras till avsett system och därefter rensas. Det finns risk att information i krypterade mejl går förlorad om eTjänstekortet går sönder eller försvinner.
Public360	Dokumentportal Public TietoEVRY Lagring sker på intern server.	Medicinsk Service	Ja	Ja	Ja	Ja	Ja	Används till styrande dokument.
Region-fastigheter VLS	Ledningssystem SharePoint 2010 Lagring sker på intern server.	Region-fastigheter	Ja	Nej	Nej	Nej	Ja	Kan hantera samtliga dokumentslag med undantag för information som kan omfattas av sekretess eller innehåller känsliga personuppgifter då behörighetsstyrning inte är anpassad för detta.
Regionservice VLS	Ledningssystem SharePoint 2010 Lagring sker på intern server.	Region-service	Ja	Nej	Nej	Nej	Ja	Kan hantera samtliga dokumentslag med undantag för information som kan omfattas av sekretess eller innehåller känsliga personuppgifter då behörighetsstyrning inte är anpassad för detta.
Samarbete, Samarbetsytan	SharePoint 2013 On-Premise Lagring sker på intern server.	Skåne-trafiken	Ja	Nej	Ja	Ja	Ja	Kan hantera samtliga dokumentslag. Även lämplig för känsliga personuppgifter och information som kan omfattas av sekretess, men inte för information som omfattas av patientdatalagen (2008:355), ändamål vård och behandling.
Samarbetsytan i SharePoint 2016 som tillhandahålls av IT	SharePoint 2016 On-Premise Lagring sker på intern server.	Region Skåne	Nej	Nej	Nej	Nej	Ja	Kan hantera samtliga dokumentslag med undantag för information som kan omfattas av sekretess eller innehåller känsliga personuppgifter då behörighetsstyrning inte är anpassad för detta. Ej avsedd för styrande dokument.
Säker lagring	SharePoint 2016 On-Premise Lagring sker på intern server.	Region Skåne	Nej	Nej	Nej	Ja	Nej	Kan användas för tillfällig lagring av information som kan omfattas av sekretess eller innehåller känsliga personuppgifter inklusive information som omfattas av patientdatalagen (2008:355) och som inte går att hantera i något av Region Skånes befintliga IT-system.

Namn	Definition och alternativa namn	Förvaltning	Arbetsflöden för granskning och godkännande	Digital signatur	Funktioner för automatisk eller halvautomatisk gallring	Lämplig för hantering av sekretess och känsliga personuppgifter	Uppfyller baskrav på metadata	Kommentar och exempel på information som kan hanteras
Teams	Office 365, Share-Point Online Lagring sker i molntjänst.	Region Skåne	Nej	Nej	Nej	Nej	Nej	Kan enbart användas för tillfällig hantering av arbetsmaterial i form av exempelvis utkast och underlag. Ytan får inte användas för information som kan omfattas av sekretess eller innehåller känsliga personuppgifter då behörighetsstyrning inte är anpassad för detta och lagring sker i molntjänst.