



## Administrativa bestämmelser för användning av WIS

### Innehåll

Systemet WIS.....	2
Bestämmelser för administration och användning av WIS.....	3
Om allmänna handlingar i WIS.....	3
Om arkivering och gallring av information i WIS.....	3
Avsluta en yta för arkivering.....	4
Gallringsbeslut hos respektive arkivbildare.....	4
Om inloggning, användare och personuppgifter i WIS.....	4
Användarens inloggningskonto och lösenord.....	5
Aktörens ansvar för användare i WIS.....	6
Hantering av personuppgifter i WIS.....	6
Om incidenthantering i WIS.....	6
Andra regler och bestämmelser att beakta vid WIS-användning.....	7
Hantering av sekretessbelagda uppgifter.....	7
Säkerhetsskyddsklassificerade uppgifter.....	7
Meddelarfriheten.....	7
Skydd för geografisk information.....	8

## Systemet WIS

WIS (Webbaserat informationssystem) är en portal för Sveriges krisberedskapsaktörer som ger möjlighet att dela information och lägesbilder med varandra före, under och efter en samhällsstörning.

Myndigheten för samhällsskydd och beredskap (MSB) förvaltar och utvecklar WIS. Myndigheter, regioner, kommuner, frivilligorganisationer och privata aktörer får använda WIS kostnadsfritt. Nya aktörer som vill använda WIS registrerar sig på [MSB:s webbplats](#).

Tidigare erfarenheter, utvecklingen i omvärlden och krisberedskapsaktörernas nya eller förändrade behov av att dela information och lägesbilder påverkar WIS. Därför pågår ständig utveckling av WIS för att möta användarnas behov och krav. I den utvecklingen ingår även de administrativa bestämmelserna som beskriver hur WIS får och ska användas.

Besök gärna [msb.se/wis](https://msb.se/wis) för mer information om WIS.

## Bestämmelser för administration och användning av WIS

De administrativa bestämmelserna reglerar WIS-aktörernas användning av WIS. En förutsättning för att få tillgång till WIS är att WIS-aktören accepterar och följer de administrativa bestämmelserna.

Administrationn av WIS är delad mellan MSB och respektive WIS-aktör. MSB utför central administration och styr vilka aktörer som ska ha tillgång till WIS. Respektive WIS-aktör administrerar sin egen användning av WIS. Följande avsnitt beskriver hur administration och ansvarsförhållanden är fördelat mellan MSB och respektive WIS-aktör och vilka förutsättningar som gäller för att använda WIS.

### Om allmänna handlingar i WIS

I tryckfrihetsförordningen (SFS 1949:105) finns regler om allmänna handlingars offentlighet. Tryckfrihetsförordningens regler om handlingsoffentlighet och möjlighet att få insyn gäller även för handlingar i elektronisk form som finns i WIS.

När en handling är upprättad blir den en allmän handling. Handlingar i elektronisk form som delas i WIS ska anses vara både upprättade och expedierade. Utgångspunkten är att en sådan handling är offentlig, om den inte innehåller några uppgifter som enligt offentlighets- och sekretesslagen (SFS 2009:400) omfattas av sekretess. WIS ska inte innehålla någon sekretessbelagd information. Det innebär i princip att all information i WIS är av karaktären att den kan nå allmänheten.

### Om arkivering och gallring av information i WIS

Varje WIS-aktör har arkivansvar för sin egen information i WIS. Det innebär att publicerad information i en yta är en allmän handling som ska:

- Registreras eller på annat sätt arkiveras i ett system hos den aktör som publicerat den.
- Registreras eller på annat sätt arkiveras i ett system hos de aktörer som besvarat eller på annat sätt behandlat informationen.

Aktörer som tagit del av information i WIS utan att besvara eller på annat sätt bearbetat informationen behöver inte registrera eller arkivera den allmänna handlingen.

I WIS kan det finnas olika typer av intern information som bara är tillgänglig för respektive WIS-aktör och som inte är allmänna handlingar, men blir allmänna handlingar vid export för arkivering. Exempel på intern information är:

- Interna anteckningar
- Interna dokument
- Interna kartposter

- Interna loggningar
- Intern begäran
- Interna kalenderinlägg

### Avsluta en yta för arkivering

Alla aktörer som enligt lag ska följa arkivlagen (SFS 1990:782) är skyldiga att exportera ut sina allmänna handlingar från WIS före radering av yta.

När en aktör inte längre aktivt deltar i en yta ska ytan avslutas och raderas. Aktören ska utse en ansvarig WIS-användare som på uppdrag av aktören genomför följande steg:

1. Aktören avslutar sitt deltagande.
2. Aktören exporterar ut allmänna handlingar för arkivering i eget system.
3. Aktören raderar ytan.

Först när alla deltagande aktörer gått igenom dess tre steg raderas ytan från WIS-databasen.

WIS-ytor där ingen aktivitet förekommit på 180 dagar inaktiveras automatiskt. Samtidigt e-postas information till deltagande aktörer att ytan avslutas inom 14 dagar. Om ytan förblir inaktiv i 14 dagar avslutas alla aktörers deltagande och ytan avslutas. När ytan varit avslutad i 30 dagar får alla deltagande aktörer e-post med påminnelse om att exportera informationen i ytan för arkivering och att radera ytan. 180 dagar efter att alla aktörer valt att radera ytan raderas den från WIS-databasen.

### Gallringsbeslut hos respektive arkivbildare

WIS-aktörer som omfattas av arkivlagen (SFS 1990:782) behöver säkerställa att respektive arkivbildare (myndighet, kommun, region etc.) fattar ett gallringsbeslut för WIS. Gallringsbeslutet hos respektive arkivbildare som omfattas av arkivlagen är nödvändigt eftersom exporter från WIS inte motsvarar det ursprungliga skicket i fråga om utseende och kontext.

Gallringsbeslutet behöver även ta hänsyn till rutinerna för att avsluta en yta i WIS för arkivering ([se avsnittet Avsluta en yta för arkivering](#)). Rutinerna beskriver när en aktörs allmänna handlingar raderas i WIS. Gallringsbeslutet behöver följaktligen förhålla sig till dessa rutiner.

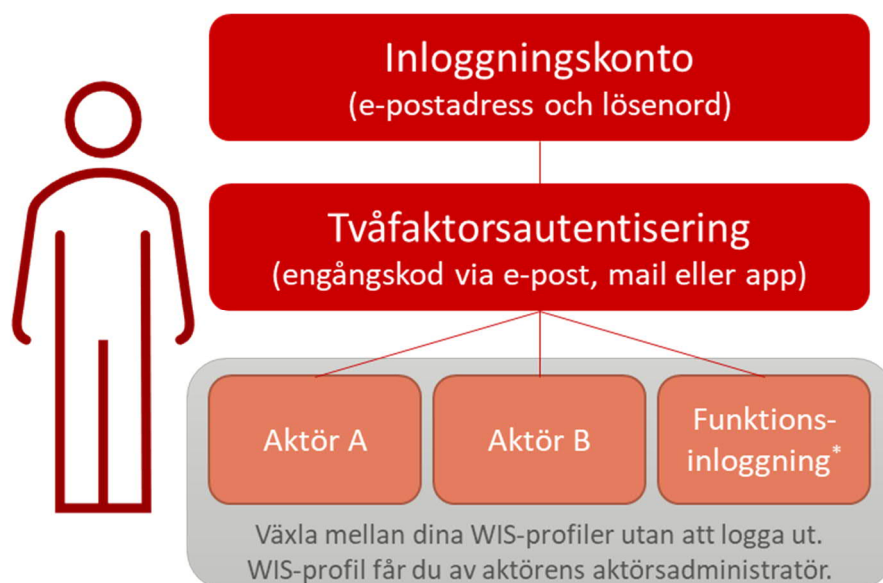
### Om inloggning, användare och personuppgifter i WIS

MSB registrerar efter ansökan nya aktörer i WIS. Registreringen inkluderar att en ny användarprofil skapas, en så kallad aktörsadministratör. Aktörsadministratören ansvarar sedan för att skapa fler användarprofiler i WIS hos den egna aktören.

För att logga in i WIS krävs ett inloggningskonto och en användarprofil. Användaren ansvarar själv för att skapa ett inloggningskonto via startsidan för WIS.

Aktörsadministratören skapar nya användarprofiler inom den egna aktören. Vid första inloggningen till WIS kopplar användaren ihop sitt inloggningskonto med användarprofilen. En användare kan koppla flera användarprofiler hos den egna aktören, eller hos andra aktörer, till sitt inloggningskonto. Det betyder att en användare kan representera flera aktörer med samma inloggningskonto.

När användaren med flera användarprofiler loggar in i WIS får användaren välja vilken användarprofil som ska användas. Det går att växla mellan användarprofiler när användaren är inloggad i WIS.



### Användarens inloggningskonto och lösenord

Inloggning i WIS sker med tvåfaktorsautentisering. Det innebär att förutom lösenord behöver användaren ange en engångskod från en autentiseringsapplikation i mobiltelefonen, sms eller e-post.

WIS ställer vissa minimikrav på lösenordets komplexitet. Lösenordet måste vara minst 16 tecken, samt innehålla tre av fyra av följande alternativ: versal, gemen, siffra, specialtecken. Det är inte möjligt att återanvända gamla lösenord.

Vad händer om man glömt sitt lösenord?

- Användaren återställer själv sitt lösenord genom att klicka "Glömt lösenord".
- Efter tre felaktiga inloggningsförsök låses kontot i tio minuter. Vid ytterligare tre felaktiga inloggningsförsök förlängs låsningstiden.

## Aktörens ansvar för användare i WIS

- Aktören ska informera egna användare om interna IT- och säkerhetsregler och dess eventuella relation till WIS. Informationen ska ges innan en användare kopplas till en aktör, alltså får en användarprofil i WIS.
- Aktören administrerar genom sin aktörsadministratör aktörens användarprofiler och behovet av fler aktörsadministratörer i WIS. Aktören bör ha interna och dokumenterade rutiner som beskriver hanteringen av användarprofiler och aktörsadministratörer.
- När användare slutar eller av annan anledning inte längre ska arbeta i WIS, åligger det aktören att omgående radera dess användarprofiler i WIS.
- Aktören ska ha interna rutiner för årlig översyn av att det bara finns behöriga användarprofiler i WIS.
- Personal med tidsbegränsad anställning eller uppdrag hos en aktör ska ges motsvarande tidsbegränsat användarprofil i WIS.
- Låst användarprofil ska öppnas först efter att identifiering och verifiering har skett av att användaren ska ha behörighet till användarprofilen.

## Hantering av personuppgifter i WIS

MSB och aktörerna i WIS har delvis samma ändamål och medel för behandlingen av personuppgifter i WIS. MSB och aktörerna i WIS har därmed huvudsakligen ett gemensamt personuppgiftsansvar. MSB är dock ensamt personuppgiftsansvarig för behandlingar av personuppgifter som utförs som en del i MSB:s aktörsadministration av WIS samt för driften och förvaltningen av WIS. Aktörerna i WIS är ensamt personuppgiftsansvarig för de behandlingar av personuppgifter som sker inom egna ytor som skapas och används i WIS.

Uppdelningen av ansvaret för personuppgifter finns dokumenterat i "*Gemensamt personuppgiftsansvar i det webbaserade informationssystemet WIS*" samt en tillhörande bilaga. Dokumenten finns på [MSB:s webbplats](#) eller kan efterfrågas hos WIS-supporten. Tillsammans utgör ett sådant arrangemang om gemensamt personuppgiftsansvar som följer av dataskyddsförordningens (GDPR:s) artikel 26. Arrangemanget återspeglar de gemensamt personuppgiftsansvarigas respektive roller och förhållanden gentemot registrerade i WIS.

Genom att ansluta sig som aktör till WIS åtar sig aktören att följa arrangemanget om gemensamt personuppgiftsansvar.

## Om incidenthantering i WIS

MSB har en WIS-support för incidenthantering och användarstöd. WIS-supporten är öppen dygnet runt alla dagar. MSB:s tjänsteman i beredskap (TIB) hanterar akuta drift- och inloggningsproblem utanför kontorstid. Vid brådskande ärenden utanför kontorstid är ett telefonsamtal det snabbaste sättet att komma i kontakt med supporten.

Kontakta WIS-supporten omgående om du upptäcker något som avviker från det normala med WIS, vid misstanke om intrång, annan säkerhetsincident eller om WIS är oåtkomligt eller funktionalitet inte fungerar som förväntat. Ring WIS-supporten på 010-240 43 00 eller e-posta till [wis@msb.se](mailto:wis@msb.se). WIS-supporten har rutiner för incidenthantering.

Personuppgiftsincidenter ska hanteras på det sätt som "*Gemensamt personuppgiftsansvar i det webbaserade informationssystemet WIS*" beskriver.

## Andra regler och bestämmelser att beakta vid WIS-användning

Utöver administrativa bestämmelser för WIS finns andra regler och bestämmelser som särskilt ska beaktas vid användning av WIS. Följande avsnitt beskriver några av dessa regler och bestämmelser.

### Hantering av sekretessbelagda uppgifter

WIS ska inte innehålla några uppgifter som omfattas av sekretess enligt offentlighets- och sekretesslagen (SFS 2009:400). En preliminär bedömning av om uppgifter i ett dokument omfattas av sekretess ska därför göras innan dokumentet laddas upp i WIS. Om osäkerhet råder om vissa uppgifter i ett dokument kan omfattas av sekretess bör dessa uppgifter maskeras (tas bort/täckas över) innan dokumentet laddas upp i WIS-systemet.

Förnyad prövning av om en handling innehåller sekretessbelagda uppgifter ska göras varje gång en handling laddas upp i WIS, laddas ner till egen plattform eller om den begärs ut.

### Säkerhetsskyddsklassificerade uppgifter

Säkerhetsskyddsklassificerade uppgifter får inte förekomma i WIS. Med säkerhetsskyddsklassificerade uppgifter avses uppgifter som rör säkerhetskänslig verksamhet och som därför omfattas av sekretess enligt offentlighets- och sekretesslagen (SFS 2009:400) eller som skulle ha omfattats av sekretess enligt den lagen, om den hade varit tillämplig.

### Meddelarfriheten

För uppgifter i WIS gäller meddelarfriheten i tryckfrihetsförordningen (SFS 1949:105) som innebär att det står var och en fritt att meddela uppgifter i vilket ämne som helst i syfte att de ska göras offentliga i en tryckt skrift. Meddelarfriheten ger även uppgiftslämnaren skydd mot efterforskning och anonymitet.

Är uppgifterna sekretessbelagda har uppgiftslämnaren rätt att tala med massmedier och muntligt lämna ut uppgifter. Däremot får uppgiftslämnaren inte skriftligen lämna ut sekretessbelagda uppgifter.

Notera att i offentlighets- och sekretesslagen (SFS 2009:400) finns regler som har företräde framför meddelarfriheten, alltså när meddelandefriheten inte gäller. I dessa fall får uppgifter inte lämnas för publicering

### Skydd för geografisk information

Det krävs tillstånd för att få utföra sjömätning, fotografering eller liknande registrering från luftfartyg (se SFS 2016:319 och SFS 2016:320). På samma sätt krävs tillstånd för att få sprida en sammanställning av geografisk information. Tillstånd kan lämnas om spridningen inte kan antas medföra skada för totalförsvaret. För en sammanställning av geografisk information som framställts endast med hjälp av fjärranalys från satellit, eller för en sammanställning av geografisk information som anger Sveriges baslinjer behövs inget tillstånd.

Försvarsmakten, Lantmäteriverket och Sjöfartsverket prövar frågor om tillstånd och kan medge undantag från tillståndskravet.