Administrativa bestämmelser för användning av WIS

Systemet tillhandahålls kostnadsfritt från MSB. Administrationen av WIS är delad. Det finns delar som MSB administrerar centralt och det finns delar som aktörerna själva administrerar.

Varje aktör i WIS ansvarar själv för att mata in, redigera och uppdatera information rörande såväl hanteringen av krisen som sina ansluta användare. Med hänsyn till detta betraktar MSB varje aktör som personuppgiftsansvarig.

MSB i egenskap av systemägare till WIS är personuppgiftsbiträde. Med personuppgiftsbiträde avses den som behandlar personuppgifter för den personuppgiftsansvariges räkning.

Enligt Dataskyddsförordningen (GDPR) ska det finnas ett skriftligt avtal mellan den personuppgiftsansvarige och personuppgiftsbiträdet. Därför krävs det att de organisationer som är anslutna till WIS tecknar ett personuppgiftsbiträdesavtal med MSB. MSB har tagit fram ett personuppgiftsbiträdesavtal som kan användas.

MSB tillhandahåller WIS via Internet. MSB lägger upp aktörer och skickar ut inloggningsuppgifter för aktörens första aktörsadministratör. Därefter är det aktörsadministratören som administrerar aktörens användare.

MSB tillhandahåller WIS-support för felanmälan och användarstöd. Supporten för WIS är öppen under kontorstid och kan kontaktas via e-post och telefon. Utanför kontorstid hanteras driftstörningar samt ärenden av enklare karaktär (exempelvis utskick av nya lösenord) med kontakt via telefon.

Aktören svarar själv för att ha en anslutning till Internet. För att systemet ska fungera ska SSL-krypterad internettrafik (https) vara möjlig genom aktörens brandvägg. Kapaciteten på aktörens internetanslutning bör vara minst 0,5 megabit per sekund för att systemet inte ska upplevas som alltför långsamt att arbeta med. Aktören ansvarar för att erforderlig kapacitet (bandbredd) mot Internet är tillgänglig. Aktören ansvarar för arbetsstationer med lämpliga webbläsare till sina användare.

Aktören administrerar genom sin aktörsadministratör sina egna användare. Detta inkluderar utdelandet av aktörsadministratörsbehörighet till en eller fler ytterligare användare, för att säkerställa redundans på rollen.

Användare skapas för närvarande i någon av standardrollerna Läsare, Skribent, Talesperson eller Redaktör.

Säkerhetsnivåer för inloggning

WIS-systemet medger två olika säkerhetsnivåer för inloggning: med eller utan förstärkt autentisering. Förstärkt autentisering innebär att användaren loggar in

MSB Myndigheten för samhällsskydd och beredskap

Postadress: 651 81 Karlstad
Besöksadress: Norra Klaragatan 18
Telefon: 0771-240 240
Telefax: 010-240 56 00
registrator@msb.se
www.msb.se
Org nr. 202100-5984

genom att ange användarnamn, pinkod och kod från säkerhetsdosa. Man behöver således ha tillgång till såväl pinkoden som säkerhetsdosan för att kunna logga in. Utan förstärkt autentisering loggar användaren in genom att ange användarnamn och lösenord, vilket ger en betydligt lägre säkerhetsnivå.

Aktören styr själv vilken säkerhetsnivå de olika kontona i WIS ska ha. Det är lämpligt att välja något av dessa handlingsalternativ:

1. Lägsta säkerhetsnivån. Alla loggar in med användarnamn och lösenord.
2. Mellannivån. Aktörens samtliga aktörsadministratörer loggar in med förstärkt autentisering. Övriga loggar in med användarnamn och lösenord.
3. Hög säkerhetsnivå. Aktörens samtliga aktörsadministratörer och redaktörer loggar in med förstärkt autentisering. Endast personer med lägsta behörighetnivån, ”användare”, loggar in utan säkerhetsdosa.

Om aktören väljer att använda förstärkt autentisering tillhandahåller MSB särskilda säkerhetsdosor med tillhörande licens mot en avgift. Aktörens kostnad är för närvarande 750 kr/dosa (exkl. moms). Varje säkerhetsdosa har en livslängd om ca 2–3 år och behöver därefter ersättas med ny.

MSB rekommenderar mellannivån, det vill säga att alla administratörer använder den förstärkta autentiseringen, eftersom de har behörighet att lägga upp nya konton och nollställa lösenord. MSB avråder från lösningar där några administratörer använder dosa och andra använder lösenord.

Regler för administration och användning av WIS

- Innan en användare ges behörighet till systemet, ska han eller hon ha fått information om aktörens egna IT-säkerhetsbestämmelser och även bestämmelserna nedan som rör användare.
- Om en användare slutar eller av annan anledning inte längre ska arbeta i systemet, åligger det aktören att plocka bort användaren ur systemet.
- Beslut om vilka användare som ska finnas i systemet ska vara dokumenterat av aktören.
- Det ska finnas utsedd personal i reserv och reservrutiner för hantering av behörighet. Antalet konton med privilegierade rättigheter bör hållas i begränsad omfattning.
- Användarkonton bör vara individuella för att upprätthålla spårbarhet i systemet.
- I särskilda fall kan användandet av funktionsinloggningar vara berättigat för att uppnå effektiv hantering vid samhällsstörningar och beredskapsarbete, exempelvis vid olika beredskapsfunktioner med rullande schema. Användningen av dessa bör vara sparsam och ska inte användas vid högre behörighetsnivåer (aktörsadministratör). Aktören ansvarar i dessa fall själv för att inloggningsuppgifter hanteras på ett säkert sätt, samt att spårbarhet mot användare dokumenteras där så behövs.
- Personal med tidsbegränsad anställning (eller konsulter) hos en aktör ska ges motsvarande tidsbegränsat konto i WIS.

- Minst en gång per år ska aktören kontrollera att bara behöriga användare är registrerade i systemet.
- De användare som ska publicera information från aktören ska läggas upp som Redaktör eller Talesperson. De användare som ska skriva anteckningar för eventuell publicering av Redaktör, ska läggas upp som Skribent. De användare som endast ska ta del av information ska läggas upp som Läsare.
- Låst användarkonto ska öppnas först efter säker identifiering av användaren.
- Innan en användare läggs upp ska denne identifieras och autentiseras.
- Varje aktör kan själv bestämma hur länge en användare kan vara inaktiv innan den blir utloggad ur WIS (standardinställning 60 minuter). Detta kan sättas av aktörsadministratörer.

Lösenord

- WIS ställer vissa minimikrav på lösenordets komplexitet. Lösenordet måste vara minst sju tecken, samt innehålla tre av fyra av följande alternativ: versal, gemen, siffra, specialtecken.
- Det är inte möjligt att återanvända gamla lösenord.
- Användare tvingas byta lösenord eller pinkod enligt det tidsintervall som aktören beslutar.
- Efter tre felaktiga inloggningsförsök låses kontot i 10 min. Efter ytterligare tre felaktiga inloggningsförsök förlängs låsningstiden.
- Om en användare glömt sitt lösenord kan ett nytt begäras via SMS till det mobilnummer som är registrerat på användaren.
- Varje aktör kan själv bestämma med vilken frekvens lösenord behöver bytas (standardinställning 90 dagar). Detta kan sättas av aktörsadministratörer.

Incidenter

- Vid misstanke om intrång eller annan incident ska MBS:s WIS-support snarast kontaktas.

Redogörelse för den lagstiftning som skall beaktas vid användning av webbaserade informationssystemet (WIS)

Bakgrund

I det uppdrag regeringen gav dåvarande Krisberedskapsmyndigheten (KBM) angående det webbaserade informationssystemet (WIS) angavs att myndigheten särskilt skulle beakta bestämmelserna i personuppgiftslagen, tryckfrihetslagen och sekretesslagen. Utgångspunkten skall, enligt regeringsuppdraget, vara att ingen sekretessbelagd information skall behandlas i systemet.

I detta dokument görs en genomgång av den lagstiftning som huvudsakligen kan tänkas vara tillämplig vid hantering av information i WIS samt hur ansvariga för systemet och användarna av systemet berörs av och bör förhålla sig till dessa bestämmelser.

Information som läggs in i systemet blir allmänna handlingar

När man lägger in dokument eller öppnar ett dagboksblad i systemet kommer detta att vanligtvis utgöra en allmän handling. Det innebär att innehållet skall kunna göras tillgängligt för allmänheten vid en begäran om utlämnande. Eftersom ingen sekretessbelagd information skall hanteras i systemet innebär det att all utlagd information kommer anses vara av sådan karaktär att man får räkna med att den kan nå allmänhetens ögon. Användare bör därför avhålla sig från att lägga in information som man inte vill skall spridas vidare. Handlingar som hanteras inom WIS kommer att utgöra allmänna handlingar hos alla de myndigheter som har möjlighet att läsa handlingen och förmedla dem vidare.

Tryckfrihetsförordningen (1949:105; TF), som är en grundlag, innehåller bl.a. regler om allmänna handlingars offentlighet. TF:s vanliga regler om handlingsoffentlighet och möjlighet att få insyn gäller även för handlingar i elektronisk form som finns i WIS-systemet.

När en handling är att anse som upprättad blir den en allmän handling. Utgångspunkten är att en sådan handling är offentlig, om den inte innehåller några sådana uppgifter som enligt sekretesslagen gör att den kan hemlighållas.

Huvudregeln är att en handling skall anses upprättad när den har expedierats, eller om den inte har expedierats men hör till ett visst ärende hos myndigheten, när ärendet har slutbehandlats hos myndigheten. Om handlingen inte har expedierats och inte kan hänföras till ett visst ärende, anses den upprättad när den har justerats av myndigheten eller har färdigställts på annat sätt. Det krävs inte något särskilt beslut för att en handling skall anses som upprättad. Detta gäller både handlingar som förs fortlöpande och ”vanliga” handlingar.

Dokument som inte utgör allmänna handlingar

Utkast, koncept och minnesanteckningar som hör till ett ärende är inte allmänna handlingar såvida de inte tas om hand för arkivering. Utkast eller koncept (s.k.

mellanprodukter, d.v.s. handlingar som är på ett tidigare framställningsstadium än den slutliga produkten) till myndighetsbeslut, skrivelser eller liknande *blir allmänna handlingar om de expedieras eller arkiveras*. Med minnesanteckningar avses promemorior och andra anteckningar som görs under beredning av ett ärende och som inte tillför ärendet några nya sakuppgifter, t.ex. föredragningspromemorior. Minnesanteckningar blir till en *allmän handling först om den tas om hand för arkivering*. Arbetsmaterial som upprättats under arbetets gång och som utväxlas mellan olika myndigheter för synpunkter *utgör inte allmänna handlingar*.

Hantering av sekretessbelagda uppgifter och krav på registrering av handlingar

Utgångspunkten är att WIS-systemet inte skall innehålla några uppgifter som omfattas av sekretess enligt Offentlighets- och sekretesslagen (2009:400). En preliminär bedömning får göras av om uppgifter i ett dokument är av sådan karaktär att de kan falla under en sekretessbestämmelse i sekretesslagstiftningen. Prövning av om uppgifter omfattas av sekretess görs dock först när en handling begärs utlämnad. En myndighet kan därför inte ta ett principiellt beslut i förväg om att viss information skall vara hemligstämplad. Om osäkerhet råder om uppgifter i ett dokument kan omfattas av sekretess bör dessa uppgifter maskeras (tas bort/täckas över) innan dokumentet läggs in i WIS-systemet.
Sekretesslagen innehåller även bestämmelser om krav på registrering av allmänna handlingar. Allmänna handlingar som har kommit in eller upprättats hos en myndighet skall som huvudregel vara registrerad hos myndigheten. Detta gäller även handlingar i elektronisk form. En handling som upprättats respektive kommit in till flera myndigheter skall således vara registrerade hos samtliga. Berörda myndigheter är ansvariga för att så sker. Myndigheterna har även ansvar att handlingarna är så ordnade att allmänheten enkelt skall kunna få tillgång till och kunna ta del av innehållet. Berörda myndigheter ansvarar för att dessa bestämmelser följs.

Meddelarfriheten

Offentliganställda har en rätt enligt TF att lämna information för publicering i media av uppgifter som finns i WIS. Det är förbjudet att ta reda på vem som lämnat uppgiften. I sekretesslagstiftningen görs vissa begränsningar av möjligheterna att lämna ut information till journalister.

Enligt TF gäller i Sverige meddelarfrihet. Meddelarfriheten består av flera moment:

- rättighet att lämna information,
- skydd för efterforskning,
- meddelarskydd.

För personer inom det offentliga är det fritt att för publicering i media lämna ut uppgifter. Denna frihet åtföljs av ett förbud för det allmänna att eftersöka vem som lämnat information till media. Den som talar med media och utnyttjar sin meddelarfrihet behöver inte avslöja sin identitet. Dessa delar av meddelarfriheten gäller bara för personer som är anställda inom det offentliga.

Meddelarskyddet innebär att en journalist aldrig behöver avslöja sina källor. Meddelarskyddet gäller både för källor som finns inom det privata och inom det offentliga. Journalisten, eller tidningen, behöver inte undersöka om en uppgiftslämnare är privatanställd eller offentliganställd för att veta att källan inte skall avslöjas.

Det finns regler i sekretesslagen som har företräde framför meddelarfriheten dvs. när meddelandefriheten bryts. Den tystnadsplikt som gäller enligt 5 kap. 8 § sekretesslagen är ett sådant exempel. Motivet till detta är att om uppgifter om t.ex. sårbarheter i myndigheters processer blir kända kan dessa utnyttjas för angrepp. Sådana angrepp skulle kunna leda till allvarliga kriser för samhället.

Iakttagande av informationssäkerhet enligt säkerhetsskyddslagen (1996:627)

I WIS skall beaktas behovet av skydd vid automatisk informationsbehandling enligt säkerhetsskyddslagen. Skydd skall finnas så att hemliga uppgifter om rikets säkerhet inte röjs, ändras eller förstörs.

Säkerhetsskyddslagen gäller vid verksamhet hos staten, kommun och landsting, bolag, föreningar och stiftelser där stat, kommun eller landsting har ett rättsligt bestämmande inflytande och enskilda om verksamheten är av betydelse för rikets säkerhet eller särskilt behöver skyddas mot terrorism. I sådana verksamheter som omfattas av lagen skall det säkerhetsskydd finnas som behövs med hänsyn till verksamhetens art, omfattning och övriga omständigheter. Vid utformningen av informationssäkerheten skall behovet av skydd vid automatisk informationsbehandling särskilt beaktas. Säkerhetsskyddet skall bland annat förebygga att uppgifter som omfattas av sekretess och som rör rikets säkerhet obehörigen röjs, ändras eller förstörs.

Uppgifter som omfattas av skydd enligt lagen och förordningen (1993:1742 resp. 1993:1745) om skydd för landskapsinformation

Det krävs tillstånd från Lantmäteriverket för bland annat upprättande av databaser med landskapsinformation och om spridning av flygbilder, kartor och andra sammanställningar av landskapsinformation.

Med landskapsinformation avses lägesbestämd information om förhållanden på och under markytan samt på och under sjö- och havsbottnen. För att få inrätta en databas med landskapsinformation över svenskt territorium krävs tillstånd av Lantmäteriverket om databasen skall föras med automatisk databehandling. Om databasen kommer att innehålla uppgifter som är av betydelse för totalförsvaret får tillstånd lämnas endast om databasens innehåll inte kan antas medföra skada för

totalförsvaret, då innehållet bara skall användas för ett visst ändamål eller om särskilda säkerhetsåtgärder vidtas. Lantmäteriverket kan bevilja bland annat myndigheter och kommuner undantag från kravet på tillstånd för att få inrätta databaser med landskapsinformation om det inte kan antas medföra skada för totalförsvaret.

Flygbilder och ”liknande registreringar från luftfartyg”, kartor i större skala än 1:100 000 och andra sammanställningar av landskapsinformation får inte spridas utan tillstånd. Tillstånd kan lämnas om spridningen inte kan antas medföra skada för totalförsvaret. Kravet på tillstånd gäller inte bilder eller andra registreringar som har framställts endast med hjälp av satelliter under förutsättning att materialet inte har ställts samman med annan landskapsinformation över svenskt territorium. Försvarsmakten, Lantmäteriverket och Sjöfartsverket får dock sprida flygbilder och kartor och det är dessa myndigheter som prövar frågor om tillstånd. De kan också medge undantag från tillståndskravet.

Hantering av personuppgifter
Varje aktör i WIS ansvarar själv för att mata in, redigera och uppdatera information rörande såväl hanteringen av krisen som sina ansluta användare. Med hänsyn till detta betraktar MSB varje aktör som personuppgiftsansvarig.

MSB i egenskap av systemägare till WIS är personuppgiftsbiträde. Med personuppgiftsbiträde avses den som behandlar personuppgifter för den personuppgiftsansvariges räkning.

Enligt Dataskyddsförordningen (GDPR) ska det finnas ett skriftligt avtal mellan den personuppgiftsansvarige och personuppgiftsbiträdet. Därför krävs det att de organisationer som är anslutna till WIS tecknar ett personuppgiftsbiträdesavtal med MSB. MSB har tagit fram ett personuppgiftsbiträdesavtal som kan användas.

Med personuppgift avses all slags information som direkt eller indirekt kan hänföras till en fysisk person som är i livet.

Med behandling av personuppgift avses varje åtgärd eller serie av åtgärder som vidtas i fråga om personuppgifter, vare sig det sker på automatisk väg eller inte, till exempel insamling, registrering, organisering, lagring, bearbetning eller ändring, återvinning, inhämtande, användning, utlämnande genom översändande, spridning eller annat tillhandahållande av uppgifter, sammanställning eller samkörning, blockering, utplåning eller förstöring.

Personuppgiftsansvarig
Den som ensam eller tillsammans med andra bestämmer ändamålen med och medlen för behandlingen av personuppgifter. I WIS är anslutna organisationer (aktörer) personuppgiftansvariga.

Personupgiftsbiträde
Den som behandlar personuppgifter för den personuppgiftsansvariges räkning. I WIS är MSB personuppgiftsbiträde. Enligt Dataskyddsförordningen (GDPR) ska det finnas ett skriftligt avtal mellan den personuppgiftsansvarige och personuppgiftsbiträdet. Därför krävs det att de organisationer som är anslutna till

WIS tecknar ett personuppgiftsbiträdesavtal med MSB. MSB har tagit fram ett personuppgiftsbiträdesavtal som kan användas.

Mål, medel och ändamål med behandlingen
Att organisationen anslutit sig till WIS innebär att MSB tillhandahåller tjänsten WIS till organisationen som en teknisk plattform där organisationen kan lagra information samt dela information med andra organisationer.
Tjänsten att tillhandahålla WIS innebär att MSB behandlar personuppgifter på organisationens vägnar.

Organisationens skyldigheter är ytterst ansvarig för att all behandling av personuppgifter sker i enlighet med dataskyddsförordningen. Organisationen ansvarar bland annat för att informera de registrerade om behandlingen, för att i nödvändiga fall hämta in samtycke från de registrerade och för att i tillämpliga fall anmäla behandlingen till tillsynsmyndigheten.

Informationsplikt
Den personuppgiftsansvarige har en omfattande skyldighet att informera de registrerade om hur deras personuppgifter kommer att behandlas. Detta gäller oavsett om samtycker krävs eller inte.
MSB ska utan dröjsmål informera organisationen om eventuella kontakter från tillsynsmyndigheten som rör eller kan vara av betydelse för MSB:s behandling av personuppgifter. MSB har inte rätt att företräda organisationen eller agera för organisationens räkning gentemot tillsynsmyndigheten eller annan tredje man.
MSB ska bistå organisationen med att ta fram information som begärts av tillsynsmyndigheten eller av en registrerad.
MSB ska bistå organisationen att fullgöra sina skyldigheter gentemot de registrerade när dessa utövar sina rättigheter enligt dataskyddslagstiftningen, exempelvis rätten till insyn, rättelse, radering, dataportabilitet etc. Detta ska ske utan oskäligt dröjsmål och utan ekonomisk kompensation, om inte parterna kommer överens om annat.

Överföring av personuppgifter till tredje land
MSB har inte rätt att överföra personuppgifter till ett land som inte är medlem i Europeiska unionen (EU) eller är ansluten till Europeiska ekonomiska samarbetsområdet (EES) i annat fall än vad som följer av dataskyddsförordningens artikel 44-46.
Utan samråd med organisationen får MSB endast behandla person-uppgifter inom en stat som ingår i EU eller är ansluten till EES.