Användarvillkor för kontoombud i unionsregistret

För att vara kontoombud i den svenska delen av unionsregistret krävs det att du godkänner användarvillkoren och så länge som du agerar som kontoombud även uppfyller dessa användarvillkor. Användarvillkoren godkänns i samband med att du fyller i din behörighetsnyckel när du loggar in första gången i unionsregistret.

Om inget annat sägs syftar uttrycken enhet och dator till den dator, surfplatta eller telefon som används för att ansluta till unionsregistret.

1. Enheter som ansluts till unionsregistret

- Vid anslutning till unionsregistret måste användaren använda en enhet som tillhandahålls av kontoinnehavaren, alternativt en privat enhet (om denna är godkänd att använda enligt kontoinnehavarens säkerhetspolicy).

2. Uppdaterade system

- Operativsystem (OS) och andra programvaror som installerats på enheten ska vara uppdaterade med de senast utgivna säkerhetsuppdateringarna.

3. Administratörs- och användarkonton

- Administratörskonton ska endast användas av behöriga personer och enbart för att installera tillåten och pålitlig programvara (se punkt 6 nedan). Enheten som används för att ansluta till unionsregistret ska generellt sett vara så välskyddad som möjligt.
- Vid anslutning till internet och unionsregistret ska användaren använda ett användarkonto i operativsystemet, inte ett administratörskonto.

4. Antimalware / Antivirus policy

- Det är användarens skyldighet att använda och uppdatera antivirusprogramvara och mjukvarubrandväggar regelbundet, åtminstone på veckobasis.
- Fullständig och djupgående skanning efter virus, s.k. spyware och malware måste konfigureras så att den utförs automatiskt åtminstone varannan vecka. Skanning ska göras med aktuell och uppdaterad antivirus- och antimalware-programvara.

EM2008, v5.1, 2017-08-11

Postadress: Box 310 • 631 04 Eskilstuna • Besöksadress Gredbyvägen 10
Telefon 016-544 23 00 • Telefax 016-544 20 99
utslappshandel@energimyndigheten.se
www.energimyndigheten.se
Org.nr 202100-5000

5. Systemlåsning

- Enheten måste ha en aktiverad skärmsläckare (eller motsvarande) som efter maximalt 15 minuters inaktivitet låser enheten. Det måste också finnas en policy som säger att en enhet aldrig får lämnas olåst utan tillsyn.

6. Kontroll över flyttbara media

- Användare får inte ansluta opålitliga USB-enheter till enheten.
- Det rekommenderas att alla USB-portar på enheten avaktiveras. Det bör åtminstone finnas en logg över anslutningar till USB-portarna.

7. Tillåten programvara (s.k. whitelisting)

- Rekommendationen är att en komplett lista över tillåten programvara som är installerad på enheten upprättas.
- Rekommendationen är att enhetens administratör säkerställer att inga andra programvaror är installerade på enheten. Detta genom att genomföra övervakning eller scanning.
- Rekommendationen är att all otillåten programvara tas bort.

8. Revision och loggning

- All åtkomst och alla anslutningar till enheten måste loggas och analyseras återkommande av administratören. Varje avvikelse måste leda till en djupare analys, även om den kan vara av det enklare slaget.

9. Säker internetanslutning

- All användning av unionsregistret måste ske genom en säker internetanslutning.
- Den säkra anslutningen måste innehålla en logisk brandvägg mellan det interna nätverk där enheten finns och internet. Brandväggen ska innehålla ett s.k. HIDS och ha antiviruskapacitet.
- Den säkra anslutningen måste begränsa åtkomst till webbplatser genom s.k. blacklisting-funktionalitet.

10. Användarkunskap

- Användare måste utbildas i att använda unionsregistret och ha förståelse för informationssäkerhetsfrågor.
- Användare ska undvika att dela användning av enheten med andra personer.
- Länkar till unionsregistret får aldrig skickas eller användas om den tagits emot.
- Europeiska kommissionen, den centrala administratören eller den nationella administratören kommer aldrig att fråga användaren efter lösenord eller efter någon form av programvara.
- Användare ska bara öppna e-postbilagor som inte kommer från unionsregistret efter en särskild bedömning kring källa och innehåll. Inga som helst bilagor med filändelserna .com, .bat, .vbs, .wsh or .exe ska öppnas.

- Om en användare har anledning att misstänka att ett mottaget e-postmeddelande med koppling till unionsregistret inte har ett ärligt syfte ska användaren kontakta den nationella administratören.
- Den nationella administratören skickar enbart e-postmeddelanden från e-postdomänerna @energimyndigheten.se och @id4.idrelay.com. Unionsregistret skickar enbart meddelanden från domänen @ec.europa.eu.
- SMS skickas enbart innehållandes SMS-kontrollkoder. Ingen annan kommunikation sker via SMS.
- Om en användare har anledning att misstänka oegentligheter i unionsregistret eller i anslutning till registret ska användaren omedelbart kontakta den nationella administratören.
- Den nationella administratören kontaktas via utslappshandel@energimyndigheten.se eller på 016 – 544 23 00 måndag – torsdag kl. 9.00 – 11.00 & 13.00 – 15.00. Vid akut läge ska användaren kontakta Energimyndighetens växel på 016 - 544 20 00.

11. Användarens datorkonfiguration

- Datorer måste konfigureras så att ”auto log-in”-funktionen inte används. Vid start eller omstart ska inloggning med lösenord alltid krävas.
- Webbläsare måste konfigureras så att användaruppgifter inte kan lagras av webbläsaren och all tillfälligt lagrad information (såsom historik, lösenord och cookies) automatiskt raderas när webbläsaren stängs ned.
- Uppstart (Boot) från CD/DVD eller USB-enheter måste undvikas genom BIOS-konfiguration. Användare ska inte ha åtkomst till BIOS-inställningar. Inställningarna ska vara skyddade av ett starkt lösenord och ett annat än login-lösenordet.
- Datorer måste konfigureras så att inga resurser kan delas med externa entiteter utanför användarens organisation (t.ex. BitTorrent).
- Datorer måste konfigureras så att användaren inte ansluter till internet med administratörsbehörigheter. Användare får inte ha möjlighet att installera programvara med kontot som ansluter till internet.

12. Användning av unionsregistret

- Lösenord som används för att logga in i unionsregistret är personliga. Alla åtgärder som genomförs i unionsregistret med ett givet e-postadress/lösenord anses vara under användarens ansvar.
- Alla behöriga användare i unionsregistret måste säkerställa att andra personer inte får ta del av inloggningsuppgifter och SMS-kontrollkoder, inklusive andra ombud eller kontoinnehavare i unionsregistret. Den centrala administratören eller nationella administratören får bara fråga användare om användarnamn via telefon. Men varken europeiska kommissionen, den centrala administratören eller den nationella administratören ska fråga efter inloggningsuppgifter.
- För att besöka unionsregistrets webbplats rekommenderas användaren att skriva in adressen till unionsregistret i webbläsarens adressfält. Om

användaren inte skriver in adressen varje gång ska användaren kontrollerar att SSL-anslutningen finns på plats (https och inte http visas i adressfältet.) och att SSL-certifikatet som visas vid klick på låsikonen i adressfältet ser ut som följer.

- Är utfärdat av "GlobalSign Extended Validation CA – SHA 256 – G3" to "ets-registry.webgate.ec.europa.eu".
- Är giltigt till 5 april 2019.
- Har följande fingerprint: " 1e 27 22 9b 1d a1 ef 1b fb 0d fb a0 c6 35 40 55 7b fd 01 64 ".

- När enheten lämnas ska användaren logga ut ur unionsregistret så att obehöriga personer inte kan få tillgång till användarens konton i unionsregistret.
- Användaren ska vidta rimliga försiktighetsåtgärder för att förhindra obehörig användning av mobiltelefoner vars telefonnummer används vid registerkommunikation.
- En mobiltelefon som tar emot en SMS-kontrollkod ska inte samtidigt användas för annan internettrafik.