| | | | | |
|---|---|---|---|---|
| | **Användarföreskrifter Informationssäkerhet – Externa parter** | | | |
| Författare (funktion, signatur) | Godkänd (funktion, signatur) | Datum | Sekretessklass | Sida (av) |
| CISO, Hans Hjertsäll | CISO, Hans Hjertsäll | 2018-10-08 | Öppen | 1(1) |

## Syfte

Användarföreskrifterna är framtagna för att belysa hur E.ON's externa parter ska förhålla sig till IT- och Informationssäkerhet. Eventuellt tilldelad fysisk utrustning ska betraktas som ett arbetsredskap och är E.ON's egendom. Föreskrifterna syftar till att informera och öka förståelsen för ditt personliga ansvar, vilka regler som gäller samt länkar till ytterligare information. Det är din skyldighet som extern part att ta del av samt följa E.ONs policy och regelverk. Överträdelse kan medföra straffansvar och disciplinära åtgärder.

### Lagstiftning

- Följa svensk lag och E.ONs policys och regler. Exempel på särskilt viktiga lagar:
  - Lag (1990:409) Skydd för Företagshemligheter
  - Dataskyddsförordningen (GDPR)
  - Säkerhetsskyddslagen (1996:627)
  - Lag om skydd för landskapsinformation (1993:1745)
  - Svenska Kraftnäts Föreskrifter om säkerhetsskydd (SvKFS 2013:1 samt 2013:2)

### E.ON policy

- E.ON's informationssäkerhetspolicy PG 05.
- E.ON äger all information som skapas eller lagras i av E.ON tillhandahållen utrustning.
- E.ON kan, utan att informera användaren, komma att ta del av sådan information om det finns anledning att misstänka brott mot uppdragsavtalet eller policys och regler.
- Kontroll av användarens IT-användning kan vidare ske för att säkra efterlevnad av gällande Informationssäkerhetspolicy och därtill knutet regelverk.
- Användare har inte rätt att utestänga E.ON från information genom tex kryptering av information med utrustning som ej tillhandahålls av E.ON.
- All IT-användning kan loggas för att skydda IT-system och användare.
- För säkerhetskyddsklassade uppdrag förutsätts att Du ger ditt samtycke till registerkontroll.

### Användning, skydd av information

- All information ska sekretessklassas enligt nivåerna nedan:
  - **Öppen**
  - **Intern**
  - **Företagshemlig**
  - **Kvalificerat Företagshemligt**
  - **Säkerhetsskyddsklassad**
- Företagshemlig information och däröver ska alltid krypteras vid lagring och överföring samt skickas med krypterad e-post.
- All information ska lagras centralt på utpekad resurs och all databehandling får endast ske på av E.ON tillhandahållen utrustning. Extern utrustning får ej kopplas in i E.ON's nät.
- Företagshemlig information och däröver, oavsett media, ska hållas under ständig uppsikt om den inte kan låsas in. Utanför E.ON's kontor ska dessa alltid hållas under uppsikt och krypteras.
- Säkerhetsfunktioner får inte avaktiveras.
- Extern anslutning till E.ON's nätverk, får endast ske via en av E.ON godkänd och tillhandahållen tjänst.
- Kvarglömda dokument i skrivare kan komma i orätta händer. Hämta dessa så fort som möjligt eller använd personlig utskriftskod.

### Etik och moral

- Du representerar E.ON och förväntas ha ett gott omdöme och korrekt uppförande, oavsett om det är vid användning av IT-tjänster eller annan tjänsteutövning.
- Användandet av kapacitetskrävande tjänster på Internet som inte behövs för verksamhetens behov är förbjudet, t.ex. nätradio, MP3, programöverföring, fildelning etc.
- Restriktivt privat användande.
- Brottslig handling, pornografi, rasism och liknande områden är förbjudet.

### Behörigheter

- All inloggning ska ske i egen behörighet. Du är personligen ansvarig för det som sker genom ditt användarkonto.
- Inloggningsinformation är personlig och ska hållas hemligt. Överträdelser ska anmälas till uppdragsgivare omgående.
- PC:n ska vara låst med lösenord när den lämnas utan uppsikt (ctrl-alt-delete) samt alltid vara utloggad och avstängd när du avslutat ditt arbetspass.

### Övrigt

- Det är din skyldighet att snarast efter uppdragsstart genomföra kravutbildning i informationssäkerhet https://disa.msb.se/ .
- Säkerhetsrelaterade incidenter ska rapporteras i anvisat system i Prevent på E.ON's intranät "Connect" eller till uppdragsgivare.
- E.ON´s tillhandahållna SIM-kort får endast användas i din personliga E.ON-utrustning
- All hantering av exempelvis USB, externa hårddiskar, mobiltelefoner etc. skall följa E.ON's regler.
- Hantera E.ON's tillgångar med försiktighet och under uppsikt. Utanför E.ON's lokaler skall informationen vara krypterad, inlåst i säkerhetsskåp eller under uppsikt.
- E.ON bedriver samhällsviktig verksamhet som intresserar många. Använd skärmfilter och prata inte om känslig information på allmän plats.

### Länkar till information/instruktioner

Mer information finns på E.ON's Intranät:

- Sökord: Informationssäkerhet

### Kontaktpersoner

- E.ON Sverige Corporate Security, CISO Hans Hjertsäll
- E.ON IT Global ServiceDesk

***Skriv under dokumentet och lämna det till din uppdragsgivare.***
***Glöm inte att ta en kopia till dig själv.***

| | |
|---|---|
| Ort och Datum | Användarnamn (KID) |
| Underskrift | Externt företagsnamn |
| Namnförtydligande | Uppdragsgivande bolag och avdelning |