SVENSKA KRAFTNÄT

Ärendenr: Svk 2020/2824-7 Version: 1.0

Informationssäkerhet för datautbyte av systemdriftsinformation

I enlighet med artikel 40.6 och 40.7 i kommissionens förordning (EU) 2017/1485 av den 2 augusti 2017 om fastställande av riktlinjer för driften av elöverförings-system

BESLUTAD

Marie Edström

SAMRÅD

Erica Niemi

RAPPORTÖR

Anders Torp

DATUM
2021-06-17

Utgåvehistorik för dokumentet

Utgåva	Datum	Kommentar
1.0	2021-06-16	Första utgåva

Innehåll

1 Ordlista

CIM	IEC CIM, Common Information Model är en internationell standardiserad informationsmodell för elkraftsystem.
DSO	Distribution System Operator, systemansvarig för distributionssystem. I Sverige regionnätägare och lokalnätägare. Ägare till s.k. icke koncessionspliktiga nät (industrinät) räknas i vissa sammanhang som DSO och har då samma skyldigheter som region- och lokalnätägare. En DSO kan äga både lokal- och regionnät.
ELCOM	ELCOM 90 är ett protokoll för utbyte av realtidsdata mellan SCADA-system. Protokollet är gammalt och ska fasas ut.
ENTSO-E	European Network of Transmission System Operator for Electricity. ENTSO-E är ett samarbetsorgan för alla TSO:er inom EU.
ICCP	Inter Control Center Protocol (ICCP/TASE.2) ett protokoll för utbyte av realtidsdata mellan SCADA-system.
KORRR	Key Organisational Requirements, Roles and Responsibilities, Viktiga organisatoriska krav, roller och ansvarsområden när det gäller datautbyte i enlighet med artikel 40.6 i kommissionens förordning (EU) 2017/1485. Metod framtagen av alla berörda TSO:er och godkänd av alla berörda tillsynsmyndigheter, dvs. Energimarknadsinspektionen (Ei) för svensk del.
Kraftsystemhubben	Kraftsystemhubben kommer vara det nav där aktörer levererar och hämtar data. Syftet med Kraftsystemhubben är att förenkla datautbytet mellan aktörer i kraftsystemet, för att på så sätt uppnå effektivare processer och arbetssätt.
Lokalnät	Här avses distributionsnät med lågspänningsslutkunder. Lokalnätägaren är DSO och ansvarar för lokalnätet. Lokalnätet är oftast radiella distributionsnät men kan innehålla spänningsnivåerna 40 – 130 kV.
OSL	Offentlighets- och sekretesslagen.
SO	System Operation Guidelines, Kommissionens förordning (EU) 2017/1485 av den 2 augusti 2017 om fastställande av riktlinjer för driften av elöverföringssystem.

TSO	Transmission System Operator, systemansvarig för överförings-systemet. I Sverige är detta Svenska kraftnät.
Överföringssystem	Det transmissionsnät som TSO förvaltar och driver.

2 Introduktion

För en säker drift av kraftsystemet behövs information om anläggningar som samverkar. Förändringar i kraftsystemet har medfört ett behov av mer omfattande datautbyte, i linje med EU-förordningen Drift av elöverföringssystem (2017/1485), även kallad System Operational Guideline (SO). SO ger ett omfattande ramverk gällande datautbytes omfattning rörande vilken information, vilka aktörer och vad aktörerna behöver komma överens om. SO kräver också att Svenska kraftnät ansvarar för att använda och tillgängliggöra data och information.

Den information som delges Svenska kraftnät via Strukturdataportalen kommer att vara tillgänglig, via begäran, för de aktörer datautbytet omfattar enligt Organisatoriska krav, roller och ansvarsområden för datautbyte (Key Organisational Requirements, Roles and Responsibilities, KORRR). Informationen avser strukturdata, realtidsdata och plandata. Det innebär exempelvis att information om anläggningar som ägs av Betydande nätanvändare (Significant Grid User, SGU) ska göras tillgänglig för anslutande Region- eller Lokalnätsägare (Distribution System Operator, DSO). Liknande ska information om DSO:s anläggningar i anslutningspunkten för en SGU komma att vara tillgänglig för SGU:n. Vidare ska även produktions-, förbruknings- och avbrottsplaner efter begäran kunna levereras av Svenska kraftnät till berörd DSO.

Svenska kraftnät vidarebefordrar strukturdata, realtidsdata och plandata till angränsande TSO:er för de nätdelar som ingår i deras observerbarhetsområde enligt gällande förordningar. Vidare ska Energimarknadsinspektionen även ha möjlighet att få tillgång till all information som utbyts.

Datautbytet omfattar olika typer av informationstillgångar från aktörer som är en del av kraftsystemet enligt definierat observerbarhetsområde. Det i sin tur ställer krav på de tekniska lösningar som behöver tillämpas för att göra datautbytet möjligt ur ett säkerhetsperspektiv. Svenska kraftnät har, i samråd med aktörer, genomfört en översyn av datautbytets informationstillgångar och gjort en bedömning av deras skyddsvärde utifrån konfidentialitet, riktighet och tillgänglighet. Med grund i lagrum har även bedömningar utifrån sekretess och säkerhetsskydd genomförts.

3 Informationsklassningsmetodik

Informationsklassning syftar till att kvantifiera skyddsvärde på informationstillgångar och skapa en bedömning för hur de ska behandlas på ett säkert sätt. Klassningen agerar även stöd i bedömningsprocessen vid utlämnande av allmänna handlingar.

Vid informationsklassningen identifieras vilka konsekvenser och skada otillräckligt skydd skulle kunna orsaka och utifrån det säkerställs att rätt åtgärder vidtas för att skydda tillgångarna. Informationsklassning avser också att undvika att tillgångarna skyddas mer än nödvändigt, vilket kan vara kostsamt och ineffektivt. Inom ramarna för datautbytet har de omfattande tillgångarna genomgått informationsklassning som medför krav på skydd som ställs på IT-system och kommunikation.

Organisationer ansvarar för eget säkerhetsarbete och utvecklar samt förvaltar därför egna klassningsmodeller. Med koppling till senare beskrivna lagrum syftas i denna rapport att klassificeringen ska på ett vedertaget sätt kunna resonera med organisationers bedömningar och säkerhetsarbete.

Standard för klassningsmodeller för säkerhetsarbete

Klassningsmodeller nyttjar aspekterna Konfidentialitet, Riktighet och Tillgänglighet (KRT). De kan i linje med standard beskrivas enligt nedan.

Konfidentialitet: Egenskapen att information inte tillgängliggörs eller avslöjas för obehöriga individer, objekt eller processer.

Riktighet: Egenskapen att informationen är korrekt samt motstå och hantera störning eller skadlig manipulation.

Tillgänglighet: Egenskapen att vara åtkomlig och användbar på begäran av ett behörigt objekt.

Den potentiella skadan inom dessa aspekter kvantifieras i konsekvensnivåer för att bilda den klassningsmatris, i Bilaga 1, som informationsklassningen utförts enligt.

3.1 Aggregerade och ackumulerade tillgångar

Aggregerade tillgångar avser då flertalet olika typer av uppgifter samlas och tillsammans skapar ett nytt skyddsvärde. Det vill säga att kombinationen av flera tillgångar kan skapa en ny summerad tillgång som är i större behov av skydd än varje enskild tillgång. Mätdata för en enskild produktionsanläggning skulle till exempel kunna bedömas att ha ett lägre skyddsvärde än samma mätdata tillsammans med dess nätmodell.

Ackumulerade uppgifter avser en ökad volym av samma tillgång där en stor mängd av den tillgången skapar ett större skyddsvärde än en liten. Ett enskilt nätschema skulle till exempel kunna bedömas att ha ett lägre skyddsvärde än alla Sveriges nätscheman tillsammans.

Om aggregerad eller ackumulerad informationen gör att en antagonist kan dra andra, eller helt nya, slutsatser av den samlade informationen än enskilda uppgifter kan det medföra att en högre klassning ska tillämpas på den samlade tillgången. Detsamma gäller om samlad tillgång möjliggör större skada med avseende på informationens tillgänglighet och riktighet.

Av förarbetena[1] till säkerhetsskyddslagen framgår att en klassning av en samling informationstillgångar inte nödvändigtvis behöver utföras i större utsträckning och med högre klassning än vad som bedöms rimligt. Detta i syfte att undvika onödiga administrativa kostnader och att försvåra verksamhetens arbete. Endast i undantagsfall, där det finns ett tydligt samband mellan uppgifterna som gör att skadan av ett röjande skulle bli mer allvarlig, kan det därför vara aktuellt att höja klassificeringen på en sammanställning av uppgifter. I denna rapport kommer definitionerna av tillgångarna att tydliggöra vilka som omfattar aggregerad eller ackumulera information.

Tekniska lösningar som IT-system och kommunikationslänkar innefattar oftast aggregerat och/eller ackumulerat skyddsvärde. Datautbytets relevanta tekniska lösningar kommer beskrivas utifrån de syften de är tänkta att betjäna och vilka datamängder de är tänkta att behandla.

4 Lagar och förordningar

Följande lagar och förordningar har legat till grund för informationsklassningen.

4.1 Säkerhetsskyddslagen

Säkerhetsskyddslagen[2] gäller för alla som till någon del bedriver verksamhet som är av betydelse för Sveriges säkerhet eller som omfattas av ett för Sverige internationellt åtagande om säkerhetsskydd. I lagtext benämns detta som säkerhetskänslig verksamhet. Lagen ställer krav på att den som bedriver säkerhetskänslig verksamhet ska genomföra säkerhetsskyddsanalys för att utreda behovet av säkerhetsskydd.

Verksamhetsutövare som lyder under säkerhetsskyddslagen ska klassificera information i enlighet med de fastställda nivåerna i säkerhetsskyddslagens andra kapitel, 5 §.

Säkerhetsskydds-klass	**Konsekvensnivå**
Begränsat hemlig	Innebär **ringa** skada för Sveriges säkerhet.
Konfidentiell	Innebär **inte obetydlig** skada för Sveriges säkerhet.
Hemlig	Innebär **allvarlig** skada för Sveriges säkerhet.
Kvalificerat hemlig	Innebär **synnerligen allvarlig** skada för Sveriges säkerhet.

Tabell 1. Säkerhetsskyddsklassificering

Tabell 1 finns ytterligare beskriven i Bilaga 2.

Det innebär att informationstillgångar som anses omfattas av säkerhetsskyddslagen ska utöver klassning med avseende på KRT även bedömas enligt ovanstående tabell och tillhörande skyddsåtgärder ska vidtas.

Informationstillgångar som omfattar säkerhetsskyddsklassificering omfattar också sekretess under offentlighets- och sekretesslagen.

4.2 Offentlighets- och sekretesslagen

Offentlighetsprincipen regleras i Sveriges grundlag och medför att allmänheten och media har rätt till insyn i statens och kommunernas verksamhet. Enkelt uttryckt har alla en grundläggande rätt att läsa de handlingar som finns hos myndigheterna. Denna rätt begränsas däremot på två sätt via Offentlighets- och sekretesslagen[3] (OSL).

För det första har allmänheten enbart rätt att läsa det som anses allmänna handlingar, och alla handlingar hos en myndighet anses inte vara allmänna. Till exempel är utkast eller koncept till en myndighets beslut eller skrivelse och andra därmed jämställda handlingar som inte har expedierats inte allmänna handlingar[4].

För det andra omfattas en del uppgifter i en myndighets handlingar av sekretess. Det innebär att allmänhetens rätt att läsa handlingarna är begränsad. Det innebär också att myndigheterna är förbjudna att lämna ut handlingarna i de delar som innehåller sådana uppgifter.

4.2.1 Allmänna handlingar

I tryckfrihetsförordningens andra kapitel finns det bestämmelser om vad som är en allmän handling och om rätten att ta del av sådana handlingar. Där finns också grundläggande bestämmelser om begränsningar av denna rätt. Kapitlet innehåller dessutom bestämmelser om hur allmänheten får tillgång till allmänna handlingar. Men enligt förordningen definieras en handling som allmän under följande förutsättningar.

- Den förvaras hos en myndighet.
- Den anses enligt särskilda regler inkommen dit eller upprättad där.

Datautbytet påverkar inte enbart organisationer som anses som myndigheter och omfattar därför informationstillgångar som inte är allmänna handlingar. Däremot medför datautbytet att Svenska kraftnät, och andra aktörer som utbytet omfattar, ska kunna få tillgång till informationen. Det medför att de informationstillgångar som Svenska kraftnät samlar in och förvaltar via portalen anses som allmänna handlingar enligt definition. För att säkerställa rätt konfidentialitet och integritet av datautbytets informationstillgångar behöver även en sekretessbedömning genomföras som del av informationsklassningens. Med andra ord bör nivå på klassning avseende konfidentialitet reflektera informationstillgångens behov av sekretess.

4.2.2 Sekretess

I offentlighets- och sekretesslagen regleras i stort sett all sekretess i det allmännas verksamhet. Innan en myndighet lämnar ut information måste en bedömning göras om informationen omfattas av sekretess eller inte. Det ska poängteras att informationsklassning i sig inte medför ett beslut om sekretess kopplat till utlämnande av handling utan enbart agerar vägledning i frågan. En förnyad sekretessbedömning måste alltid genomföras för enskilda utlämnanden. Om en myndighet väljer att inte lämna ut en handling med hänvisning till sekretess och lagrum markeras detta genom en sekretessmarkering.

En sekretessmarkering medför däremot inte att en informationstillgång inte kan lämnas ut alls. En myndighet kan lämna ut en sekretessbelagd handling med förbehåll som begränsar möjligheterna att använda den information som finns i handlingen.

Informationsklassningen i detta dokument omfattar en sekretessbedömning av datautbytets informationstillgångar och rapporten avser att förmedla klassningens förhållande till medgivande och förbehåll vid utlämnande.

4.2.3 Utlämnande med medgivande

Som tidigare nämnt medför informationsklassning inte ett beslut om sekretess, och ny sekretessbedömningen krävs vid varje begäran om utlämnande. Däremot avser denna rapport att generalisera klassningsmetodiken för att återspegla ett förhållningssätt till sekretess och utlämning av enskilda handlingar med koppling till datautbytet för att underlätta förståelsen.

- Informationstillgångar som, utifrån konfidentialitet, bedöms kunna orsaka **ingen** skada om de röjs anses generellt inte som sekretessbelagd. Handlingen kan därför lämnas ut enligt prövningens utfall. Om informationen ursprungligen kom från en aktör och vid prövning bedöms som allmän handling avser Svenska kraftnät att inte efterfråga medgivande innan utlämnande för denna klassning.
- Informationstillgångar som, utifrån konfidentialitet, bedöms kunna orsaka **begränsad** eller **allvarlig** skada om de röjs anses kunna omfattas av sekretess. Handlingen kan därför lämnas ut enligt prövningens utfall. Om informationen ursprungligen kom från en aktör och vid prövning bedöms som allmän handling avser Svenska kraftnät att efterfråga medgivande innan utlämnande för dessa klassningar.
- Om aktören anser att handlingen inte bör lämnas ut bör man tillhandahålla en egen sekretessbedömning. Om Svenska kraftnät delar den bedömningen blir informationen sekretessbelagd och en bedömning gällande utlämnande med förbehåll krävs. Om Svenska kraftnät inte delar aktörens sekretessbedömning kommer handlingen lämnas ut enligt offentlighetsprincipen.
- Informationstillgångar som, utifrån konfidentialitet, bedöms kunna orsaka **synnerligen allvarlig** skada om de röjs anses i regel omfatta säkerhetsskydd och är då därmed också sekretessbelagd. Sådan informationstillgång kommer inte att lämnas ut utan förbehåll och det är inte heller säkert att informationen kan lämnas ut även med förbehåll.

4.2.4 Utlämnande med förbehåll

Ett förbehåll är en formell överenskommelse som inkluderar villkor som råder för att utlämnandet av sekretessbelagd information från en myndighet ska vara möjligt. Dessa villkor är menade att förebygga att informationen sprids vidare till en annan person eller utnyttjas till ändamål för att orsaka skada.

Ett sekretessförbehåll är inget avtal[5]. Det bygger istället på en överenskommelse om konfidentialitet mellan enskild person och myndighet som medför tystnadsplikt[6]. Myndigheten lämnar enbart ut informationen om förbehållet godtas[7]. Ett förbehåll är ett beslut som fattas ensidigt av myndigheten och som kan överklagas[8].

För att ett sekretessförbehåll ska vara giltigt måste det framgå vilken information som handlingen avser, vem den lämnas ut till och under vilka villkor. En myndighet kan inte i förbyggande syfte besluta om förbehåll som gäller en eller flera informationstillgångar och inte heller flera personer eller en hel organisation[9]. En myndighet måste därför fatta ett nytt beslut om förbehåll för varje enskilt utlämnande för varje enskild person.

- Vid begäran om utlämnande av sekretessbelagd informationstillgång avser Svenska kraftnät att efter prövning bedöma ifall informationen kan lämnas ut med förbehåll eller inte. Om informationen ursprungligen kom från en aktör och vid prövning bedöms kunna lämnas ut med förbehåll kommer Svenska kraftnät, i samråd med berörd aktör, utforma förbehållet.

  Ifall en aktör istället anser att informationen inte kan lämnas ut även med förbehåll kommer en motivering att efterfrågas. Det kan till exempel vara en hänvisning till affärssekretess. Om Svenska kraftnät godtar motiveringen kommer informationen inte att lämnas ut med motivering samt hänvisning till sekretess och lagrum.

4.3 Informationssäkerhet för samhällsviktiga och digitala tjänster

Lag om informationssäkerhet för samhällsviktiga och digitala tjänster[10] (NIS-lagen) omfattar elnätsverksamhet. Där ställs det krav på bland annat följande.

- Egen riskbedömning och egen nivå på säkerhetsåtgärder.
- Anmälan att företaget ska stå under tillsyn.
- Incidentrapportering.
- Att möjliggöra tillsyn annars vite.
- Tillsyn kan resultera i åtgärdsföreläggande (får förenas med vite).
- Säkerhetsåtgärder – Skyldigheter för leverantörer av samhällsviktiga tjänster.

Gällande säkerhetsåtgärder ska datautbytet realiseras i enlighet med NIS-lagen där leverantörer av samhällsviktiga tjänster, i syfte för att säkerställa leveransen av de samhällstjänsterna, ska upprätthålla följande praxis.

- Systematiskt och riskbaserat informationssäkerhetsarbete ska bedrivas.
- Riskanalyser, med tillhörande åtgärdsplan, som ska ligga till grund för val av säkerhetsåtgärder ska genomföras.
- Ändamålsenliga och proportionella tekniska och organisatoriska åtgärder för att säkerställa en nivå på säkerheten i förhållande till risk ska vidtas.
- Lämpliga åtgärder för att förebygga och minimera verkningar av incidenter för att upprätthålla kontinuitet ska vidtas.

Svenska kraftnät bedriver ett övergripande säkerhetsarbete i enlighet med NIS-lagen. Bedömningarna av tillgångarnas skyddsvärde avser att rätt krav ställs på de tekniska lösningar som möjliggör datautbytet.

4.4 Dataskyddsförordningen

Personuppgiftslagstiftningen har som syfte att skydda individers integritet och att skydda privatpersoner från att företag och organisationer använder personuppgifter på ett oetiskt sätt eller som handelsvara. Syftet är dock inte att förbjuda eller försvåra behandling av data som innehåller personuppgifter.

Dataskyddsförordningen[11] (GDPR) ska efterlevas av företag, organisationer och myndigheter. Enligt förordningen är en personuppgift varje uppgift som avser en identifierad eller identifierbar fysisk person. Definitionen är mycket bred och innebär att alla uppgifter som går att koppla till en (levande) person anses vara en personuppgift och datautbytet kommer att omfatta vissa sådana uppgifter.

Grundreglerna i dataskyddsförordningen är att personuppgiftsbehandling måste ha ett tydligt ändamål och det måste finnas en laglig grund för behandlingen. De vars personuppgifter behandlas har enligt förordningen också vissa rättigheter som de kan åberopa. Dessa rättigheter är rätten att begära ett registerutdrag, rätten att bli bortglömd, rätt till begränsning av behandling, rätt till att göra invändningar, rätt till portabilitet av personuppgifter och rätten att få sina personuppgifter rättade.

Den enskildes rättigheter är i flera fall juridiskt underordnade annan lagstiftning vad gäller myndigheters behandling av personuppgifter. Till exempel kan en person inte åberopa principen om ”rätten att bli bortglömd” hos Skatteverket. Denna princip är också underordnad arkivlagen och principerna om att en myndighets arbete ska kunna följas upp och granskas, vilket är en orsak till att det mesta på en myndighet utgör allmän handling och inte får raderas utan gallringsbeslut från Riksarkivet.

Svenska kraftnät behandlar personuppgifter i enlighet med dataskyddsförordningen. Inom ramen för datautbytet blir personuppgifter, och lagring av dessa, aktuellt vid användandet av Kraftsystemhubben i form av uppgifter för inloggning och användare. En korrekt bedömning av personuppgifters skyddsvärde medför att rätt säkerhetskrav ställs på de system som omfattar sådan information.

5 Informationstillgångar

Svenska kraftnät har genomfört en kartläggning över vilka informationstillgångar som datautbytet kommer att omfatta. Svenska kraftnät har även, i samråd med aktörer, genomfört en bedömning av dessa informationstillgångars skyddsvärde samt förhållande till OSL och Säkerhetsskyddslagen.

Aktörer som är i behov av stöd i sitt eget säkerhetsarbete vid införandet av datautbytet kan efterfråga utlämnande av resultatet från kartläggning- och bedömningsarbetet. Förfrågan om utlämnande skickas till datautbyte@svk.se.

6 Tekniska lösningar

För att genomföra datautbytet krävs ett par tekniska lösningar. I huvudsak IT-system för förvaltning av strukturdata och kommunikationslösningar för insamling av mätvärden. Svenska kraftnät vill ge en inblick i säkerhetsbedömningen av dessa tänkta lösningar.

6.1 Kraftsystemhubben och strukturdataportalen

Svenska kraftnät utvecklar kraftsystemhubben som ett nav där aktörer levererar och hämtar data. Som del av hubben utvecklas även en underliggande plattform kallad strukturdataportalen. Kraftsystemhubben kommer att agera plattform för utbyte av transaktionsdata medan strukturdataportalen hanterar strukturdata.

Kraftsystemhubben och strukturdataportalen agerar gränssnitt mot Svenska kraftnäts interna processtödssystem (back-end). Systemet kommer att omfatta grundläggande funktionalitet som:

- Användarinloggning (multifaktorsautentisering)
- Ärendehantering (Skapa, ändra, återkoppla, godkänna, avvisa)
- Datafilsuppladdning (CIM)

Den information som portalen ska hantera ligger till grund för beslut i vissa kärnprocesser och funktioner i Svenska kraftnäts verksamhet. Systemet har däremot inte en direkt koppling till dem vilket medför att en obehörig användare inte direkt kan orsaka processerna och funktionerna skada.

Överföringen av datautbytets uppgifter ska ske manuellt via ärendehantering och handläggare. Svenska kraftnät bedömer att risken för obehörig åtkomst från hubben och portalen till säkerhetskänsliga funktioner hanteras via ärendehanteringen och risken för fel i uppgifter hanteras genom handläggarens bedömning.

Svenska kraftnät har genomfört en särskild säkerhetsskyddsbedömning, i enlighet med PMFS 2019:2, av IT-systemet som medför att rätt säkerhetskrav ställs. En förnyad särskild säkerhetsskyddsbedömning behöver genomföras vid säkerhetspåverkande förändringar av systemet. Om till exempel ny information tillkommer som medför nya hot, risker och sårbarheter för systemet eller om användningen av systemet ökar för att stödja ytterligare verksamhetsprocesser och funktioner.

6.2 Kommunikation

Utbyte av realtidsmätvärden kommer inte att ske via strukturdataportalen. I portalen delas enbart mätningarnas strukturdata men systemet hanterar inte mätvärden i sig. För att möjliggöra utbyte av realtidsmätvärden krävs andra kommunikationslösningar.

6.2.1 Fiberförbindelse

Svenska kraftnät nyttjar idag fiberförbindelser för utbyte av realtidsdata med vissa aktörer. Detta sker via protokollen ICCP eller Elcom, även om Elcom fasas ut. Svenska Kraftnät tillämpar idag ett IT-system för denna typ av kommunikationslösning som även fortsättningsvis kommer att tillämpas innanför och utanför observerbarhetsområdet.

En förnyad säkerhetsskyddsbedömning behöver genomföras vid säkerhetspåverkande förändringar av systemet. Svenska kraftnät bedömer att datautbytet inte orsakar förändringar och befintlig kommunikationsutrustning kommer inte att påverkas.

6.2.2 Ny kommunikationslösning

Fiberförbindelser kan vara komplicerade och kostsamma att implementera för mindre anläggningsägare. Svenska kraftnät utvecklar därför en ny kommunikationslösning som ska vara en praktisk och kostnadsmässigt fördelaktig leveransmöjlighet för mindre och anläggningar.

Svenska Kraftnät utvecklar ett nytt IT-system för den nya kommunikationslösningen. Lösningen är tänkt att bestå av en sändningsenhet i stationer som mottar realtidsmätvärden från olika givare i stationerna, en mottagningsenhet hos Svenska Kraftnät, en databas samt olika säkerhetsmekanismer. Sändningsenheten skickar dessa realtidsdata vidare till mottagningsenheten hos Svenska Kraftnät på ett säkert sätt över ett bärarnät. Databasen har förmåga att tolka och analysera data och skickar sedan data vidare till bakomliggande system. De mottagande systemen använder olika egna säkerhetsmekanismer som tillsammans med säkerhetsarkitektur och nätverkssegmentering stärker skyddet för bakomliggande system som anses vara samhällskritiska. Dessa mottagande system kommer också att kompensera för eventuellt dålig datakvalitet.

Svenska kraftnät har genomfört en särskild säkerhetsskyddsbedömning, i enlighet med PMFS 2019:2, av kommunikationslösningen som medför att rätt säkerhetskrav ställs i de tekniska riktlinjerna. Exempel på säkerhetskrav som kan komma att ingå är:

- Sändningsenheten behöver rätt nivå av fysiskt skydd.
- Sändningsenhet och mottagningsenhet behöver autentisera varandra.
- Datakanalen mellan sändningsenhet och mottagningsenhet behöver säkerställa konfidentialitet, riktighet och tillgänglighet.
- Systemet bör inte lita på inkommande data utan kontroll.
- Systemet bör konstrueras så att dataintrång försvåras och upptäcks och att konsekvenserna av dataintrången begränsas.

Ytterligare information rörande kommunikationslösningens utformning och implementering kommer att tillhandahållas efter behov.

Bilaga 1 – Klassningsmatris

Tabell 2 omfattar den värdering som bedömning av informationstillgångars skyddsvärde har utförs ifrån.

Skada	**Konfidentialitet (K)**	**Riktighet (R)**	**Tillgänglighet (T)**
Ingen	Information där förlust av konfidentialitet innebär **ingen** skada för egen eller annan organisation, eller på enskild individ.	Information där förlust av riktighet innebär **ingen** skada för egen eller annan organisation, eller på enskild individ.	Information där förlust av tillgänglighet innebär **ingen** skada för egen eller annan organisation, eller på enskild individ.
Begränsad	Information där förlust av konfidentialitet innebär **begränsad** skada för egen eller annan organisation, eller på enskild individ.	Information där förlust av riktighet innebär **begränsad** skada för egen eller annan organisation, eller på enskild individ.	Information där förlust av tillgänglighet innebär **begränsad** skada för egen eller annan organisation, eller på enskild individ.
Allvarlig	Information där förlust av konfidentialitet kan innebära **allvarlig** skada för egen eller annan organisation, eller på enskild individ.	Information där förlust av riktighet kan innebära **allvarlig** skada för egen eller annan organisation, eller på enskild individ.	Information där förlust av tillgänglighet kan innebära **allvarlig** skada för egen eller annan organisation, eller på enskild individ.
Synnerligen allvarlig	Information där förlust av konfidentialitet kan innebära **synnerligen allvarlig** skada för egen eller annan organisation, eller på enskild individ.	Information där förlust av riktighet kan innebära **synnerligen allvarlig** skada för egen eller annan organisation, eller på enskild individ.	Information där förlust av tillgänglighet kan innebära **synnerligen allvarlig** skada för egen eller annan organisation, eller på enskild individ.

Tabell 2. Klassningsmatris

Bilaga 2 – Säkerhetsskyddsklassificering

Tabell 3 omfattar säkerhetspolisens matris för säkerhetsskyddsklassificering.

Säkerhets-skyddsklass	**Konsekvensnivå**	**Konsekvenser**
Begränsat hemlig	Innebär **ringa** skada för Sveriges säkerhet.	**Ringa** negativa konsekvenser som är begränsade till att påverka, försvåra eller störa den nationella förmågan i mindre omfattning.
Konfidentiell	Innebär **inte obetydlig** skada för Sveriges säkerhet.	**Påtagliga** negativa konsekvenser för den nationella förmågan, om än i begränsad omfattning, som äventyrar, vållar skada, hindrar, underlättar för en antagonist eller innebär större avbrott.
Hemlig	Innebär **allvarlig** skada för Sveriges säkerhet.	**Allvarliga/betydande** negativa konsekvenser, av stor omfattning eller av väsentlig art, som innebär ett direkt hot mot den nationella förmågan, om än mot avgränsade funktioner. Svårt att återställa.
Kvalificerat hemlig	Innebär **synnerligen allvarlig** skada för Sveriges säkerhet.	**Synnerligen** allvarliga negativa konsekvenser av stor omfattning, under lång tid, som utgör ett direkt hot mot den nationella förmågan. Konsekvenserna är inte begränsade till enstaka funktioner. Mycket svårt att återställa.

Tabell 3. Säkerhetsskyddsklassificering[12]

En broschyr med denna matris kan hämtas från säkerhetspolisens hemsida.

Fotnoter

[1] Regeringens proposition 2017/18:89, s. 66.

[2] Säkerhetsskyddslagen (2018:585).

[3] Offentlighets- och sekretesslagen (2009:400).

[4] Tryckfrihetsförordningen 2 kap. 12 §.

[5] JO 1994/95 s. 574.

[6] Brottsbalken 20 kap. 3 §.

[7] JO 2905-07.

[8] TF 2:19.

[9] JO 1992/93 s. 197.

[10]Lag (2018:1174) om informationssäkerhet för samhällsviktiga och digitala tjänster.

[11] Dataskyddsförordningen (2016/679).

[12] Säkerhetspolisen, 2019, Vägledning i säkerhetsskydd – Informationssäkerhet.