SÄKERHETSSKYDDSARBETE OCH BEREDSKAPSHÖJANDE ÅTGÄRDER FÖR TELEKOM

ROBUSTHETSVECKAN
MAJ 2022

Jimmy Persson
Utveckling- och säkerhetschef
Jimmy.persson@ssnf.org
08-214 640

Säkerhetsskyddsarbete och beredskapshöjande åtgärder

- **Säkerhetsarbetet för nätägare**
  - Säkerhetstriangeln
  - Driftsäkerhet, IT-säkerhet, Informationssäkerhet, Säkerhetsskydd
- **Säkerhetsskyddsarbete**
  - Delar att hantera
  - Säkerhetskyddsanalysen
  - Nyheter: 1 december 2021
- **Vi sammanfattar säkerhetsarbetet**

- **Beredskapshöjande åtgärder**

Jimmy Persson
Utveckling- och säkerhetschef
Jimmy.persson@ssnf.org
08-214 640

IoT/OT-SÄKERHET

SÄKER FYSISK FÖRBINDELSE

SITE FÖR KRITISK VERKSAMHET

SÄKERHETSARBETE FÖR NÄTÄGARE AV DIGITAL INFRASTRUKTUR

LAGRUM

Driftsäkerhet
IT-säkerhet
Informationssäkerhet

Säkerhetsskydd

Lagen om elektronisk kommunikation **(LEK) 2003:389**
Förordning om elektronisk kommunikation **2003:396**

PTS Driftsäkerhetsföreskrifter
PTSFS 2015:2 och **PTSFS 2020:1**

Offentlighets- och sekretesslagen **(OSL) 2009:400**

Lag (2006:544) om kommuners och regioners åtgärder inför och vid extraordinära händelser i fredstid och höjd beredskap

Lag (1992:1403) om totalförsvar och höjd beredskap

Lag (2018:1174) om informationssäkerhet för samhällsviktiga och digitala tjänster (NIS)

Säkerhetsskyddslagen **2018:585**
Säkerhetsförordning **2021:955**
PMFS 2022:1 Säkerhetspolisens föreskrifter om säkerhetsskydd
PTSFS 2021:2 Post- och telestyrelsens föreskrifter om säkerhetsskydd

Risk- och sårbarhetsanalys På anläggningstillgångar 1

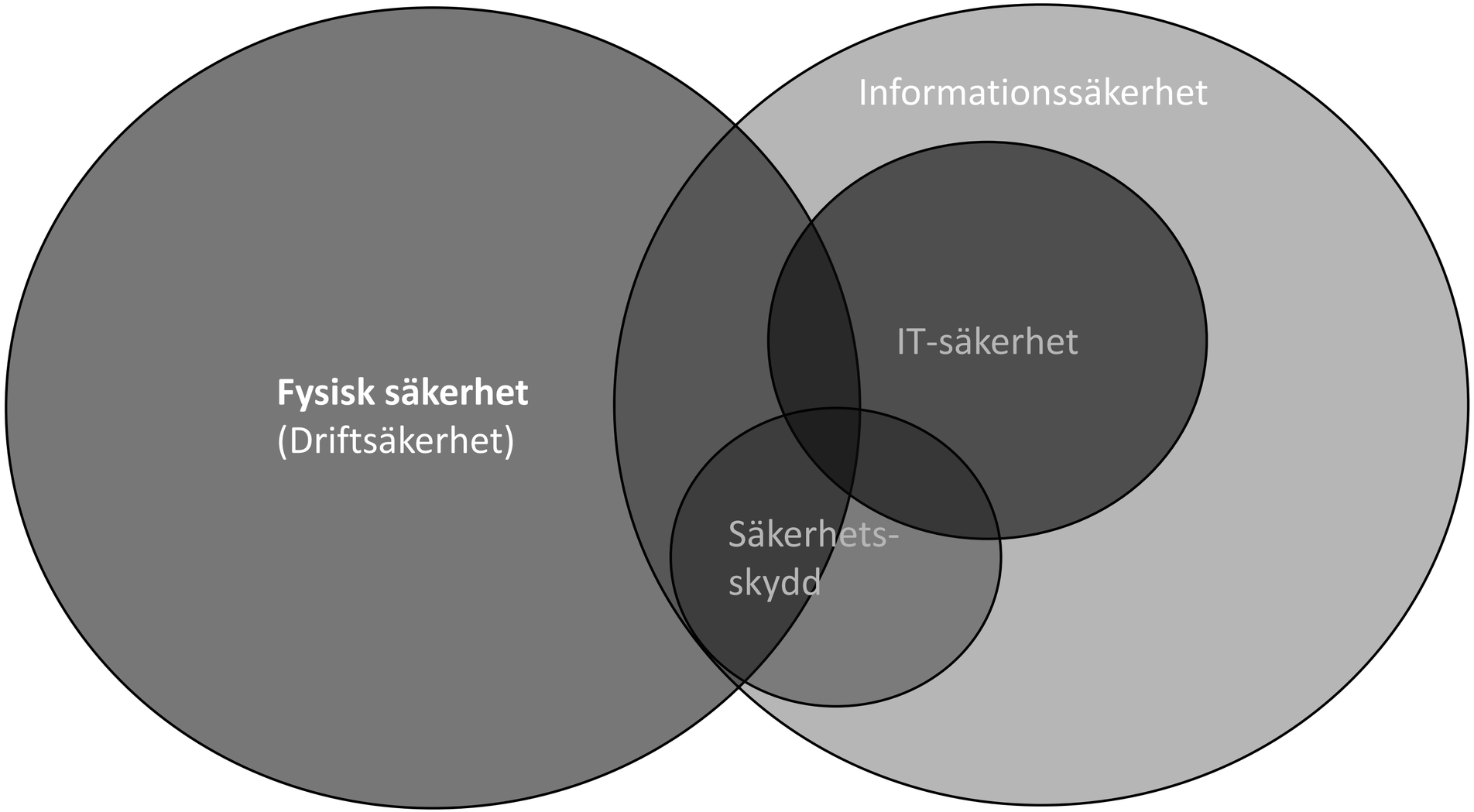
Konsekvensanalys på Verksamhetsdel nätdrift 2

Säkerhetsskyddsanalys 3

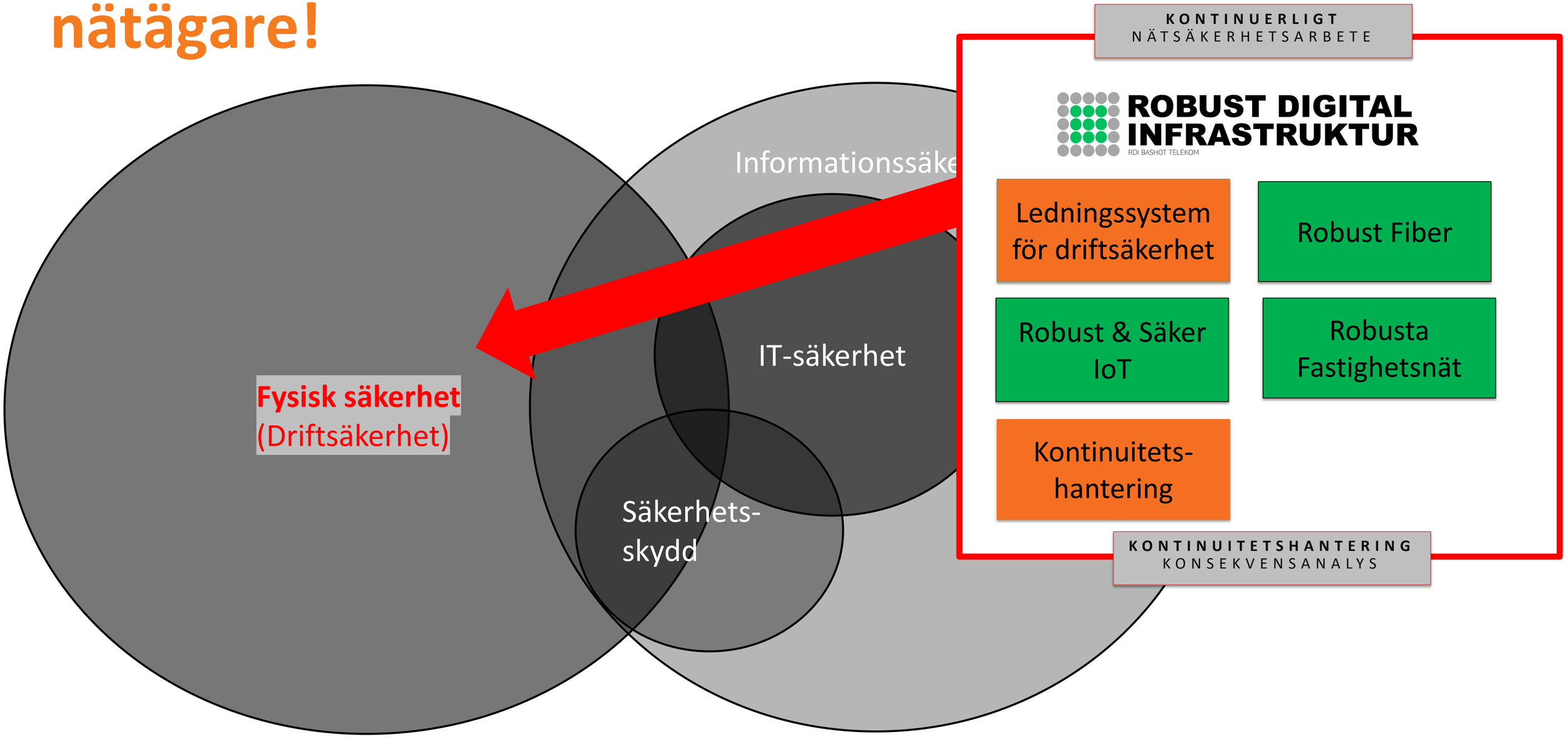
VERKTYG

Åtgärder av olika slag
- Direkta åtgärder
- Schemalagda åtgärder
- Periodiska åtgärder
- Förbättringar
- Förstärkningar

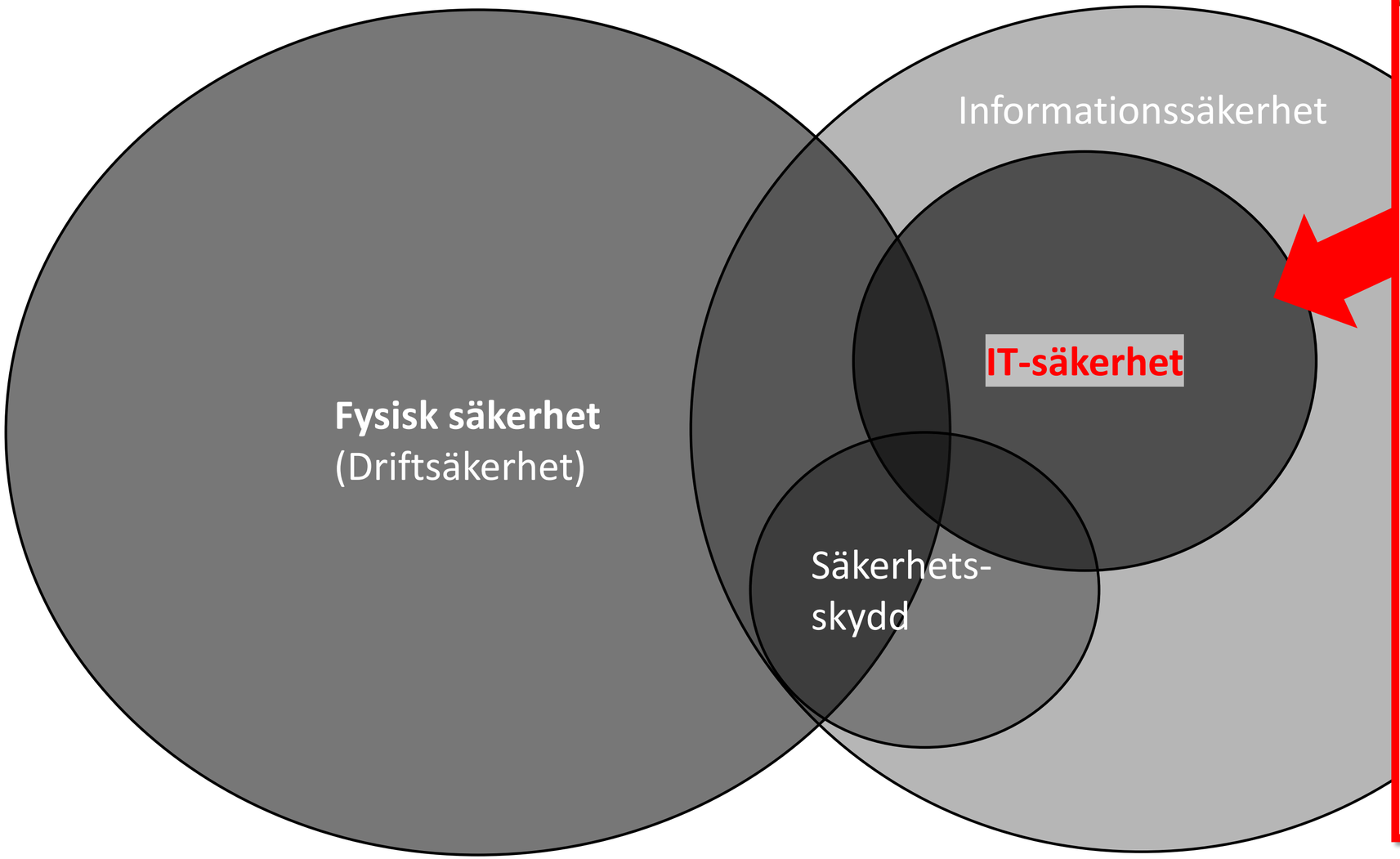
Säkerhetsområden för nätägare att förhålla sig till!



Säkerhetsområden för nätägare!



Säkerhetsområden för nätägare!



Säkerhetsområden för Stadsnätsverksamhet!

SVENSKA STADSNÄTS FÖRENINGEN

Säkerhet- och informationssäkerhetspolicy
Stockholm 2022-01-01

Säkerhetsansvarig: Jimmy Persson, 073-274 26 15
Teknisk support: Rasmus Rahm, 070-531 47 10

Säkerhet- och informationssäkerhetspolicy för Svenska Stadsnätsföreningens kansli

Säkerhetskultur

Policyn definierar ramen för hanteringen av säkerhet/ informationssäkerhet och gäller alla medarbetare i Svenska Stadsnätsföreningen och definierar vår säkerhetskultur.

Säkerhetskulturen ska kännetecknas av att arbeta med rätt nivå av säkerhet och integritet, både den fysiska säkerheten och den information som vi hanterar. Vi ska arbeta enligt ställda krav med stort fokus på hållbara lösningar. Vår Säkerhet- och informationssäkerhetspolicy är grundläggande i vårt arbete för att ständigt förbättra vår egen och våra medlemmars säkerhet och intresse.

Syfte

Syftet med denna policy är både en vägledning samt förhållningssätt av användande av Stadsnätsföreningens säkerhetskultur och IT-utrustning. Den ska även bidra till att säkerställa att Stadsnätsföreningens resurser, data, samt personuppgifter hanteras på ett tillbörligt och lagligt sätt.

Medarbetare är skyldig att följa denna policy. Medarbetare är skyldig att följa lagar samt rutiner och policys som upprättats i syfte att följa lagstiftning gällande hantering av personuppgifter och säkerhetsskydd.

Sunt förnuft ska gälla och en allmän och alltid närvarande vaksamhet kring säkerhetshot ska tas i beaktande.

IT-utrustning: Dator och mobiltelefon

- Datorer, telefoner, surfplattor som är ägda av Svenska Stadsnätsföreningen, ska vara konfigurerade enligt framtagen konfigurering. Konfigurering består av att dator ska innehålla:
- Dator: Office 365, Norton 360 Antivirus, Dropbox, Adobe reader, Lime CRM, Konferensapplikationer , SIM-kort.
- Mobiltelefon: E-post, Kalender, Virusskydd, SIM-kort.
- Det är ok att installera egen programvara på dator. Det ska alltid beaktas risken att Malware inte installeras. Samtliga programvaror ska alltid hållas uppdaterad.
- Privat surfing är ok med gott omdöme. Vid frågor vad som anses vara tillåtet rådfråga Säkerhetsansvarig.

Svenska Stadsnätsföreningen | *Swedish Local Fibre Alliance*
Drottninggatan 94 | 111 36 Stockholm | Sweden
Phone: +46 8 214 930 | E-mail: kansli@ssnf.org | www.ssnf.org

TLP:WHITE

Sekretess och säkerhetsklassning av information

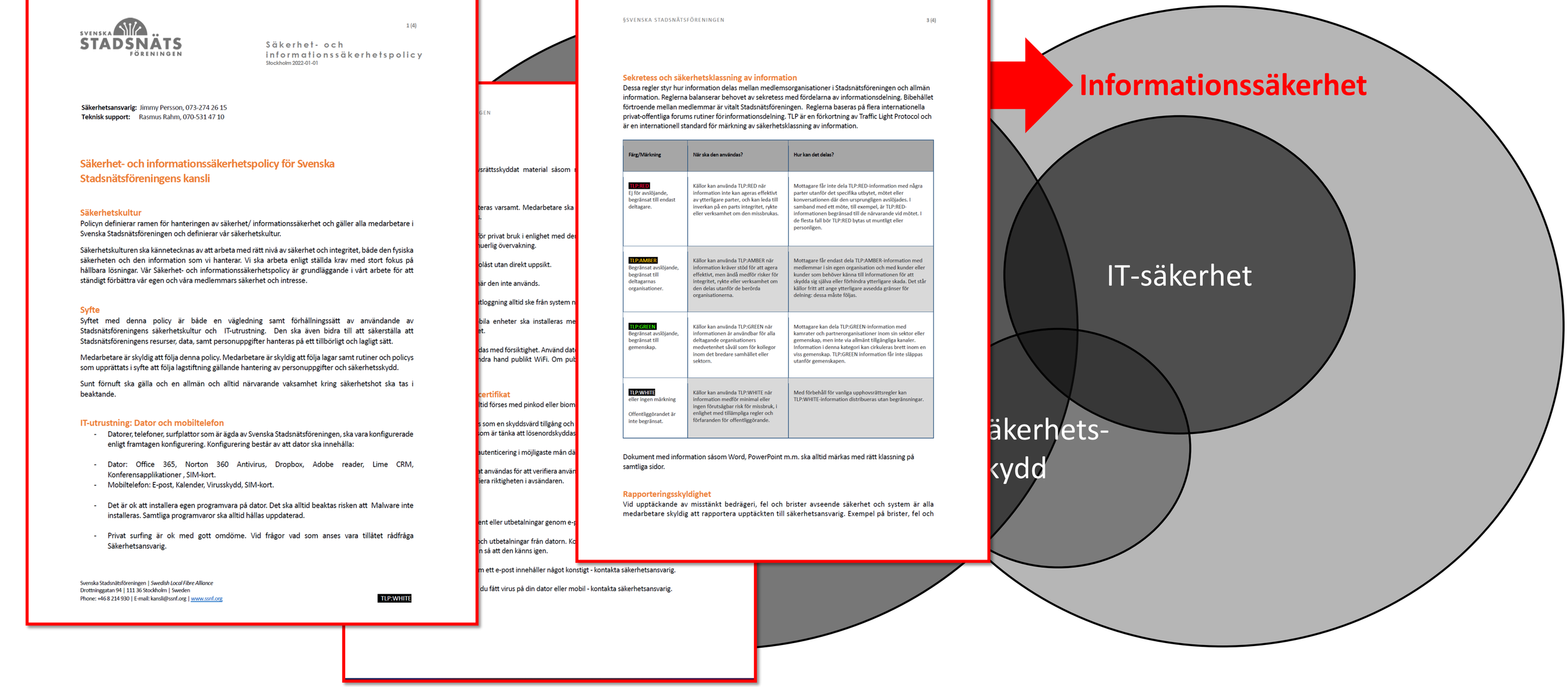
Dessa regler styr hur information delas mellan medlemsorganisationer i Stadsnätsföreningen och allmän information. Reglerna balanserar behovet av sekretess med fördelarna av informationsdelning. Bibehållet förtroende mellan medlemmar är vitalt Stadsnätsföreningen. Reglerna baseras på flera internationella privat-offentliga forums rutiner för informationsdelning. TLP är en förkortning av Traffic Light Protocol och är en internationell standard för märkning av säkerhetsklassning av information.

Färg/Märkning	När ska den användas?	Hur kan det delas?
TLP:RED Ej för avslöjande, begränsat till endast deltagare.	Källor kan använda TLP:RED när information inte kan ageras effektivt av ytterligare parter, och kan leda till inverkan på en parts integritet, rykte eller verksamhet om den missbrukas.	Mottagare får inte dela TLP:RED-information med några parter utanför det specifika utbytet, mötet eller konversationen där den ursprungligen avslöjades. I samband med ett möte, till exempel, är TLP:RED-informationen begränsad till de närvarande vid mötet. I de flesta fall bör TLP:RED bytas ut muntligt eller personligen.
TLP:AMBER Begränsat avslöjande, begränsat till deltagarnas organisationer.	Källor kan använda TLP:AMBER när information kräver stöd för att agera effektivt, men ändå medför risker för integritet, rykte eller verksamhet om den delas utanför de berörda organisationerna.	Mottagare får endast dela TLP:AMBER-information med medlemmar i sin egen organisation och med kunder eller kunder som behöver känna till informationen för att skydda sig själva eller förhindra ytterligare skada. Det står källor fritt att ange ytterligare avsedda gränser för delning: dessa måste följas.
TLP:GREEN Begränsat avslöjande, begränsat till gemenskap.	Källor kan använda TLP:GREEN när informationen är användbar för alla deltagande organisationers medvetenhet såväl som för kollegor inom det bredare samhället eller sektorn.	Mottagare kan dela TLP:GREEN-information med kamrater och partnerorganisationer inom sin sektor eller gemenskap, men inte via allmänt tillgängliga kanaler. Information i denna kategori kan cirkuleras brett inom en viss gemenskap. TLP:GREEN information får inte släppas utanför gemenskapen.
TLP:WHITE eller ingen märkning Offentliggörandet är inte begränsat.	Källor kan använda TLP:WHITE när information medför minimal eller ingen förutsägbar risk för missbruk, i enlighet med tillämpliga regler och förfaranden för offentliggörande.	Med förbehåll för vanliga upphovsrättsregler kan TLP:WHITE-information distribueras utan begränsningar.

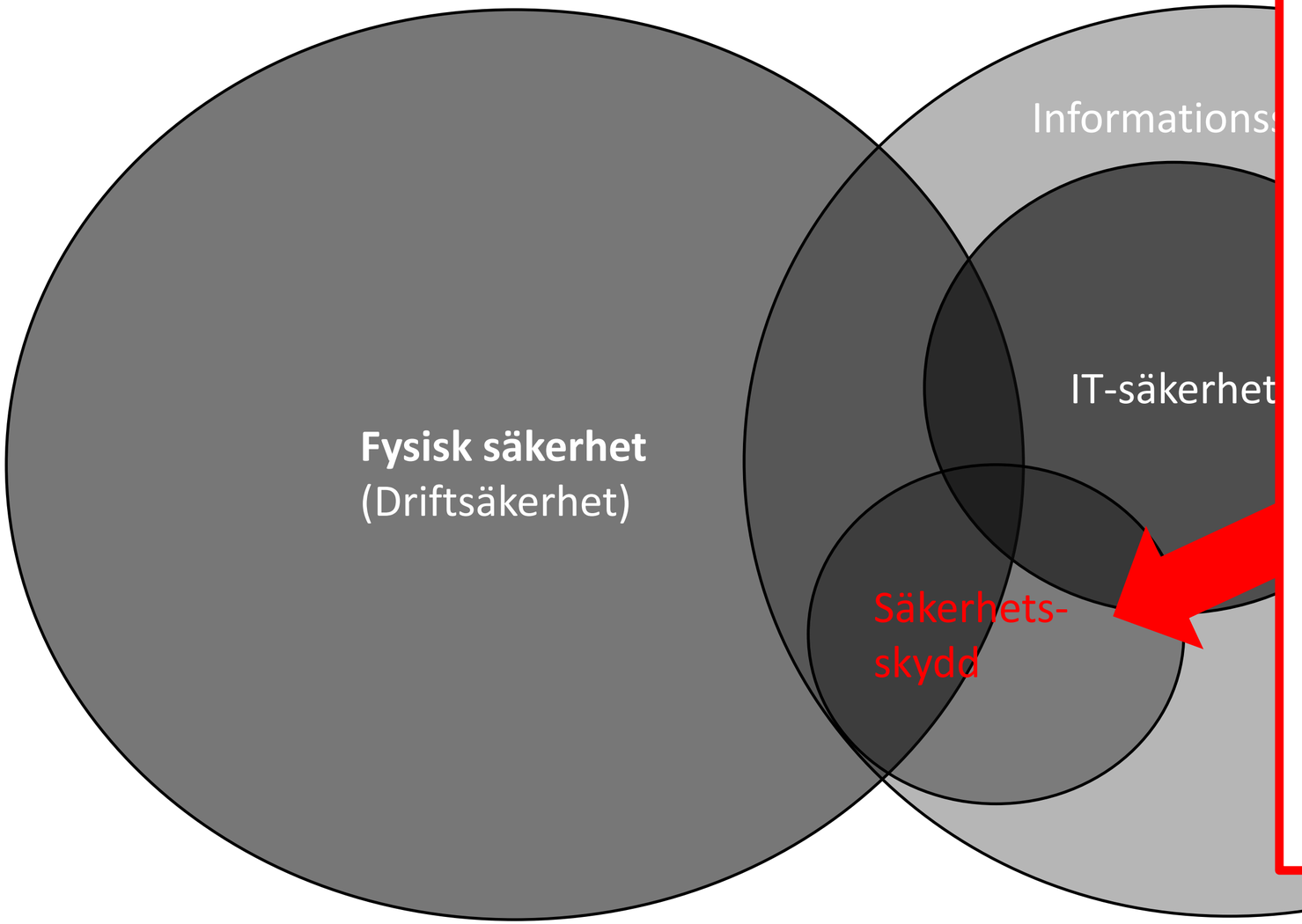
Dokument med information såsom Word, PowerPoint m.m. ska alltid märkas med rätt klassning på samtliga sidor.

Rapporteringsskyldighet

Vid upptäckande av misstänkt bedrägeri, fel och brister avseende säkerhet och system är alla medarbetare skyldig att rapportera upptäckten till säkerhetsansvarig. Exempel på brister, fel och



Säkerhetsområden för Stadsnätsverksamhet!



- Skydd av säkerhetskänslig verksamhet **(VAD)**
- mot spioneri, sabotage, terroristbrott och andra brott som kan hota verksamheten **(MOT)**
- samt skydd i andra fall av säkerhetsskydds-klassificerade uppgifter **(VAD)**
- Ett system av förebyggande åtgärder **(HUR)**

Sveriges säkerhet
och
Säkerhetsskyddsarbete

Vad är säkerhetsskydd?

- Skydd av säkerhetskänslig verksamhet **(VAD)**
- mot spionerи, sabotage, terroristbrott och andra brott som kan hota verksamheten **(MOT)**
- samt skydd i andra fall av säkerhetsskyddsklassificerade uppgifter **(VAD)**
- Ett system av förebyggande åtgärder **(HUR)**

Informationssäkerhet

Personalsäkerhet

Säkerhetsskyddsavtal

Extern aktör

Fysisk säkerhet

”Säkerhetskänslig verksamhet”

Begreppet säkerhetskänslig verksamhet omfattar såväl militär som civil verksamhet och är oberoende av om verksamheten bedrivs av det offentliga eller av enskilda aktörer.

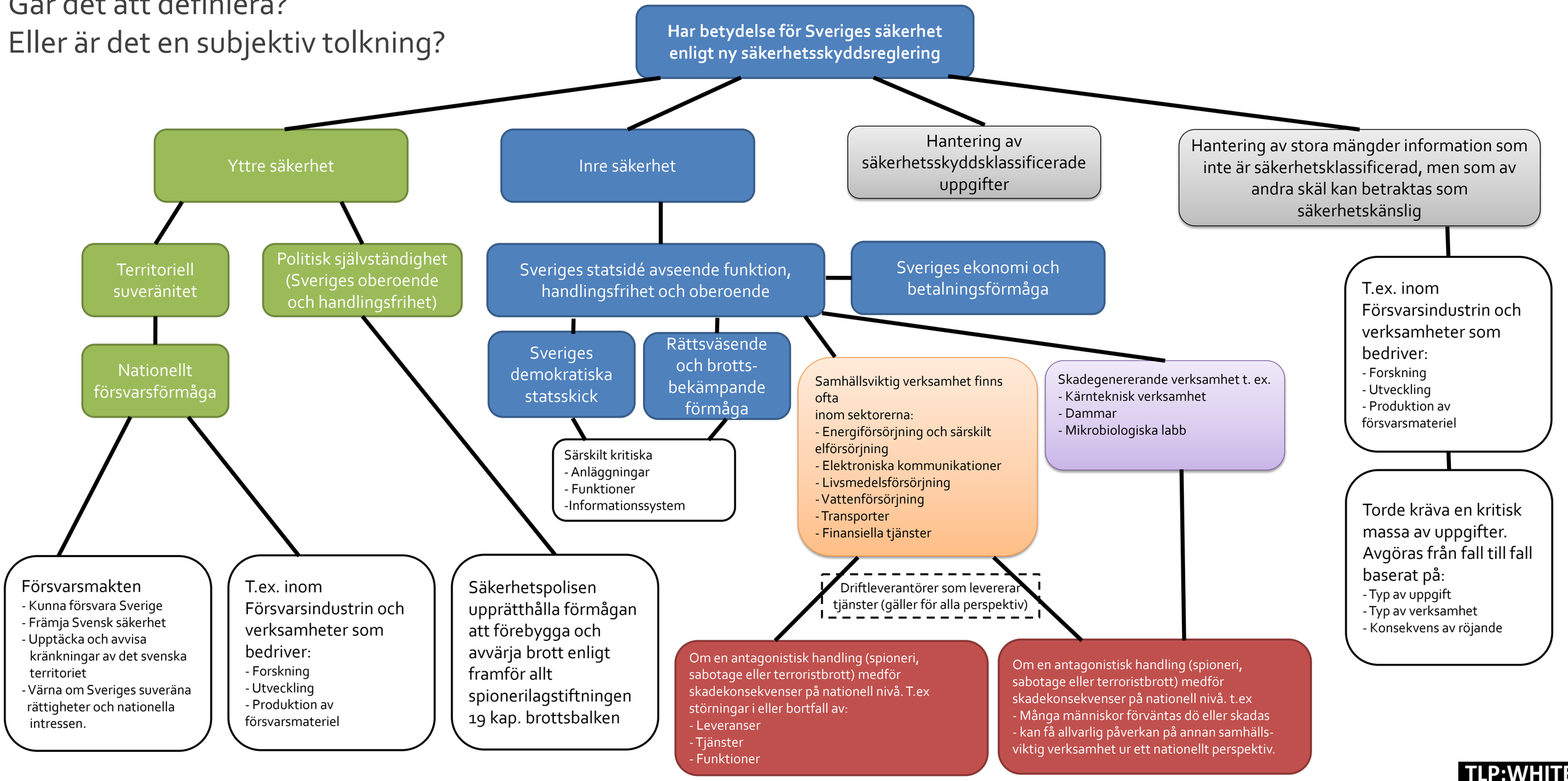
Inom många verksamheter är **endast en viss del, tillgång eller funktion av betydelse för Sveriges säkerhet.** Verksamhetsutövaren måste då noggrant analysera vilka delar som är säkerhetskänsliga så att säkerhetsskyddsåtgärderna inte görs onödigt omfattande men inte heller missar delar som omfattas av säkerhetsskyddslagens krav.

Utgångspunkten är att verksamheten ska ha **direkt betydelse för Sveriges säkerhet** men även verksamhetsutövare som till exempel levererar **driftstjänster <u>såsom data- och telekommunikation</u>**, kan anses bedriva verksamhet som är av betydelse för Sveriges säkerhet. Det kan då vara den samlade betydelsen som indirekt aktualiserar behovet av säkerhetsskydd även om de enskilda uppdragen sedda var och en för sig inte är säkerhetskänsliga.

TLP:WHITE

Sveriges säkerhet

Går det att definiera?
Eller är det en subjektiv tolkning?



TLP:WHITE

Säkerhetsskyddslag (2018:585)

Grundläggande förståelse

Skydd av säkerhetskänslig verksamhet mot spionerі, sabotage, terroristbrott och andra brott som kan hota verksamheten samt skydd i andra fall av säkerhetsskydds-klassificerade uppgifter.

SÄKERHETSSKYDD

Skyldigheter för den som bedriver säkerhetskänslig verksamhet

Säkerhetsskyddsanalys
(Utreda behovet av säkerhetsskydd samt dokumentera det)

Planera och vidta de säkerhets-Skyddsåtgärder som behövs med hänsyn till verksamhetens art och omfattning, förekomst av säkerhets-klassificerade uppgifter och övriga omständigheter.

Kontrollera säkerhetsskyddet i den egna verksamheten, anmäla och rapportera sådant som är av vikt för säkerhets-skyddet och i övrigt vidta de åtgärder som krävs.

Så långt det är möjligt ska säkerhets-skyddsåtgärderna utformas så att de inte medför någon skada eller annan olägenhet för andra allmänna eller enskilda intressen.

Säkerhetskänslig verksamhet

Verksamhet som är av betydelse för Sveriges Säkerhet eller omfattas av ett för Sverige för-pliktande internationellt åtagande om säkerhets-skydd.

Informationssäkerhet

1) Förebygga att säkerhetsklassificerade uppgifter obehörigen röjs, ändras, görs otillgängliga eller förstörs

2) Förebygga skadlig inverkan i övrigt på uppgifter och informationssystem som gäller säkerhetskänslig verksamhet.

Fysisk säkerhet

1) Förebygga att obehöriga får tillträde till områden, byggnader och andra anläggningar eller objekt där de kan få tillgång till säkerhetsskydds-klassificerade uppgifter eller där säkerhetskänslig verksamhet i övrigt bedrivs.

2) Förebygga skadlig inverkan på sådana områden, byggnader, anläggningar eller objekt som avses i 1

Personalsäkerhet

1) Förebygga att personer som inte är pålitliga från säkerhetssynpunkt deltar i en verksamhet där de kan få tillgång till säkerhetsskyddsklassificerade uppgifter eller i en verksamhet som av någon annan anledning är säkerhetskänslig.

2) Säkerställa att de som deltar i säkerhetskänslig verksamhet har tillräcklig kunskap om säkerhetsskydd.

Säkerhetsskyddsklassificerade uppgifter

Uppgifter som rör säkerhetskänslig verksamhet och som därför omfattas av sekretess enligt offentlighets-och sekretesslagen (2009:400) eller som skulle ha omfattas av sekretess enligt lagen, om den hade varit tillämplig.

Säkerhetsskyddsklassificering

Uppgifter ska delas in i säkerhetsskyddsklasser utifrån den skada som ett röjande av uppgiften kan medföra för Sveriges säkerhet.

Motsvarande om de omfattas av ett internationellt åtagande om de inte redan har klassificerats. Utifrån skada som ett röjande av uppgiften kan medföra för Sveriges förhållande till skadan.

- Kvalificerat hemlig vid en synnerligen allvarlig skada
- Hemlig vid en allvarlig skada
- Konfidentiell vid en inte obetydlig skada
- Begränsad hemlig vid endast ringa skada

Skyddslagen (2010:305)
(Inte en rak koppling men kan påverka)

Åtgärder till förstärkt skydd för byggnader, andra anläggningar, områden och andra objekt mot sabotage, terroristbrott, spionerі samt röjande i andra fall av hemliga uppgifter som rör totalförsvaret och grovt rån.

Säkerhetsskyddsavtal

1) Det i upphandlingen förekommer säkerhetsskyddsklassificerade upp-gifter i säkerhetsklassen konfidentiell eller högre, eller
2) Upphandlingen i övrigt avser eller ger leverantören tillgång till säkerhets-känslig verksamhet av motsvarande betydelse för Sveriges säkerhet.

Säkerhetsprövning

Säkerhetsklass 1

1) I en omfattning som inte är ringa får del av uppgifter i säkerhetsskydds-klassen kvalificerat hemlig, eller

2) till följd av sitt deltagande i verk-samheten har möjlighet att orsaka synnerligen allvarlig skada för Sveriges säkerhet.

Säkerhetsklass 2

1) I en omfattning som inte är ringa får del av uppgifter i säkerhetsskydds-klassen hemlig,

2) I ringa omfattning får ta del av uppgifter i säkerhetsskyddsklassen kvalificerat hemlig, eller

3) till följd av sitt deltagande i verk-samhet har möjlighet att orsaka allvarlig skada för Sveriges säkerhet.

Säkerhetsklass 3

1) Får del av uppgifter i säkerhetsskyddsklassen konfidentiell,

2) I ringa omfattning får ta del av uppgifter i säkerhetsskyddsklassen hemlig, eller

3) till följd av sitt deltagande i verk-samhet har möjlighet att orsaka allvarlig skada för Sveriges säkerhet.

TLP:WHITE

Säkerhetsskydd

- Säkerhetsskyddslag (2018:585)
- Säkerhetsskyddsförordning (2021:955)
- Säkerhetspolisens föreskrifter om säkerhetsskydd, PMFS 2022:1
- Post och telestyrelsens föreskrifter om säkerhetsskydd, PTSFS 2021:2

TLP:WHITE

Säkerhetsskyddsarbetet

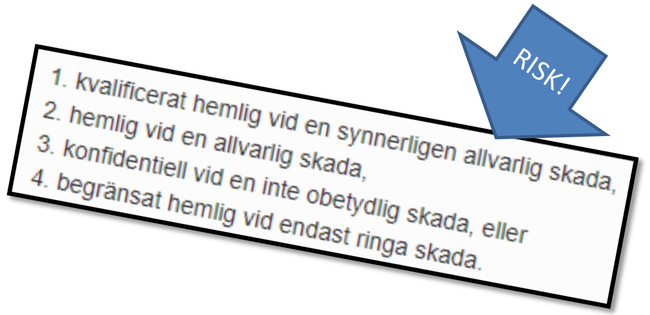
1)	**Upprätta säkerhetsskyddsanalys**	*(2 kap. 1 §första st.)*
2)	Planerat och vidtagit säkerhetsskyddsåtgärder	(2 kap. 1 §andra st.)
3)	Säkerhetsskyddsklassificera uppgifter	(2 kap. 5 §)
4)	Anmäl säkerhetskänslig verksamhet	(2 kap. 6 §första st.)
5)	Tillsätt Säkerhetsskyddschef direkt underställd ledning	(2 kap. 7 §)
6)	Säkerhetspröva personal, etc.	(3 kap. 1-4 §§)
7)	Placerat personal i säkerhetsklass	(3 kap. 6-9 §§)
8)	Ingå relevanta säkerhetsskyddsavtal	(4 kap. 1 §)

6 §

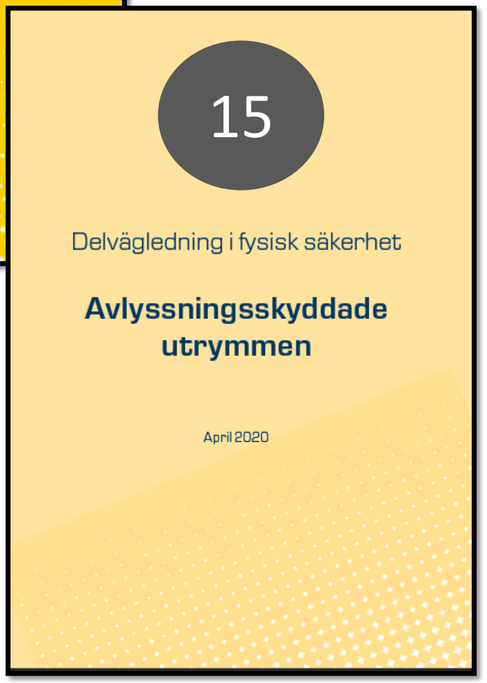
Paragrafen, som är ny, innehåller bestämmelser om anmälningsskyldighet för verksamhetsutövare. Övervägandena finns i avsnitt 8.2.

Enligt *första stycket* ska en verksamhetsutövare anmäla att den bedriver säkerhetskänslig verksamhet. Anmälan ska ske utan dröjsmål efter det att den säkerhetskänsliga verksamheten påbörjas. För den som redan bedriver säkerhetskänslig verksamhet vid tidpunkten för ikraftträdandet av paragrafen innebär kravet att anmälan ska ske utan dröjsmål efter ikraftträdandet.

Enligt *andra stycket* ska en verksamhetsutövare anmäla till tillsynsmyndigheten när den säkerhetskänsliga verksamheten har upphört. Även denna anmälan ska göras utan dröjsmål.



Stöd i arbetet från Säkerhetspolisen



Säkerhetspolisen

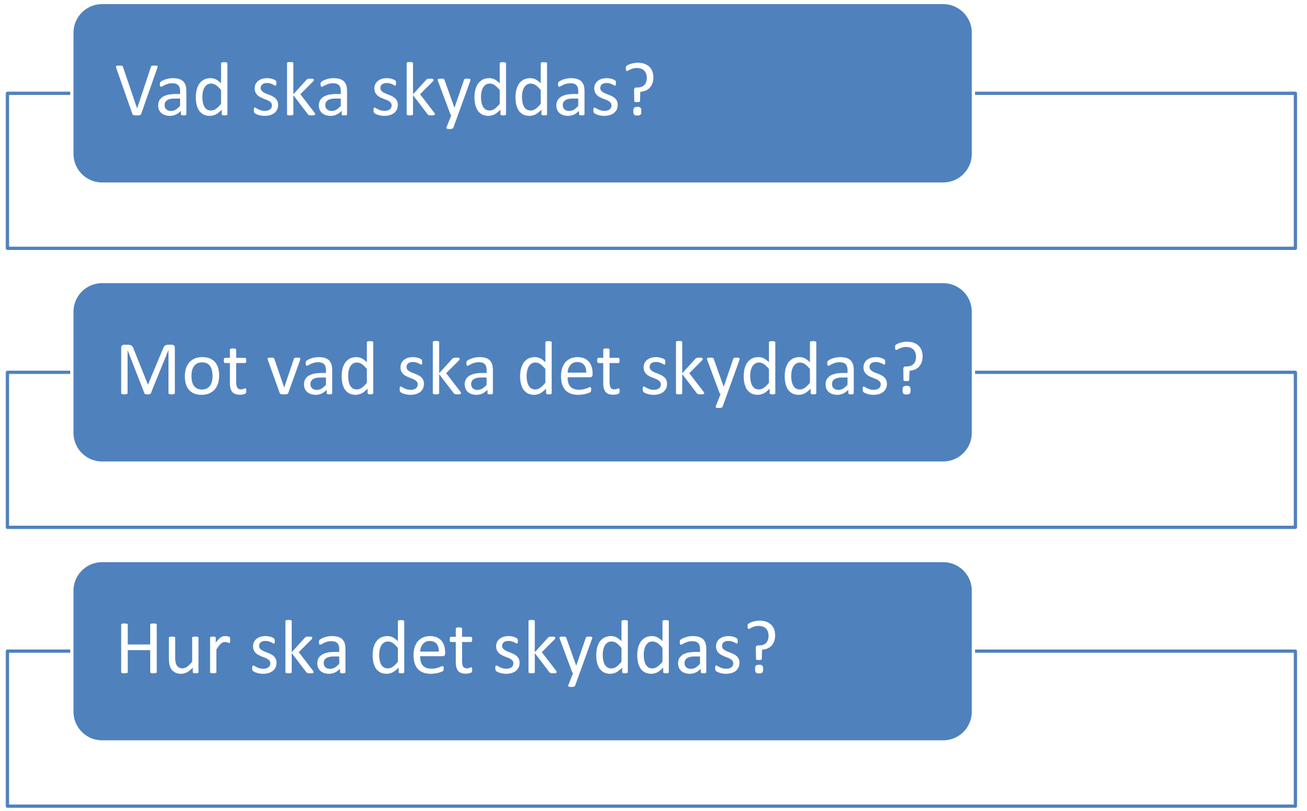
Säkerhetsskyddsanalys
SÄPOs metod

IoT/OT-SÄKERHET

SÄKER FYSISK FÖRBINDELSE

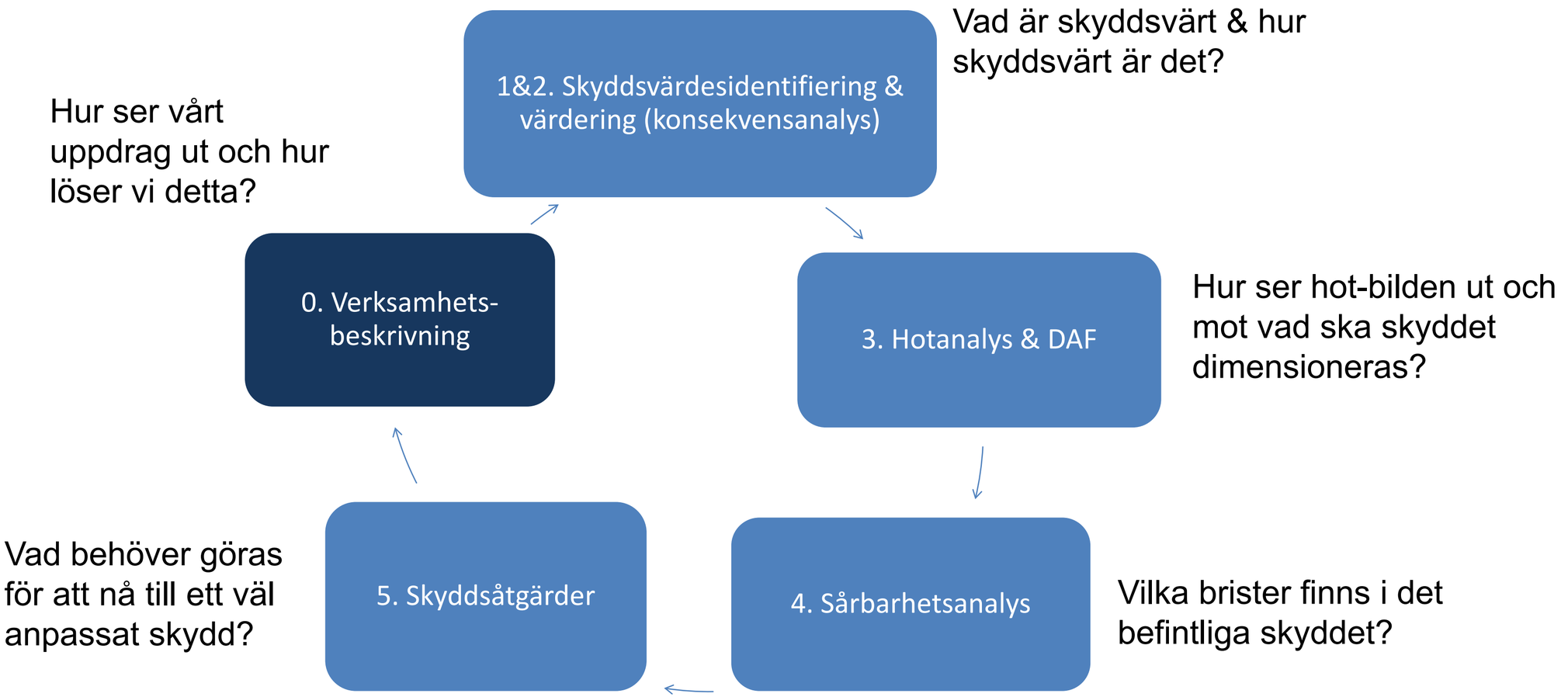
SITE FÖR KRITISK VERKSAMHET

En väl genomförd säkerhetsanalys ger svar på frågorna:



Källa: Säkerhetspolisen

Viktiga komponenter i en säkerhetsanalys



Källa: Säkerhetspolisen

Viktiga övergripande komponenter i en säkerhetsanalys

Figur 1: Säkerhetspolisens modell för att ta fram en säkerhetsskyddsanalys.

Källa: Säkerhetspolisen

Viktiga övergripande komponenter i en säkerhetsanalys

Figur 1: Säkerhetspolisens modell för att ta fram en säkerhetsskyddsanalys.

Källa: Säkerhetspolisen

Verksamhetsbeskrivning

Figur 1: Säkerhetspolisens modell för att ta fram en säkerhetsskyddsanalys.

Källa: Säkerhetspolisen

Verksamhetsbeskrivning

Konsekvenskategori

Vad ska skyddas?

2 § Verksamhetsutövaren ska övergripande beskriva sin verksamhet och specificera vilka delar av verksamheten som är av betydelse för Sveriges säkerhet utifrån kategorierna

- Sveriges yttre säkerhet
- Sveriges inre säkerhet
- Nationellt samhällsviktig verksamhet
- verksamhet av betydelse för Sveriges ekonomi
- verksamhet som kan generera skada på annan säkerhetskänslig verksamhet

0

Källa: Säkerhetspolisen

Verksamhetsbeskrivning

Förslag på aktiviteter

Vad ska skyddas?

I Beskriv övergripande verksamheten samt dess mål och syfte

II Identifiera säkerhetskänslig verksamheten med utgångspunkt i den övergripande beskrivningen av verksamheten, och utifrån verksamhetsutövarens instruktion eller motsvarande styrdokument.

Besvara frågorna om det till någon del bedrivs verksamhet som:

- hanterar säkerhetsskyddsklassificerad uppgift,
- Omfattas av ett för Sverige förpliktande internationellt åtagande om säkerhetsskydd eller
- är av betydelse för Sveriges säkerhet.

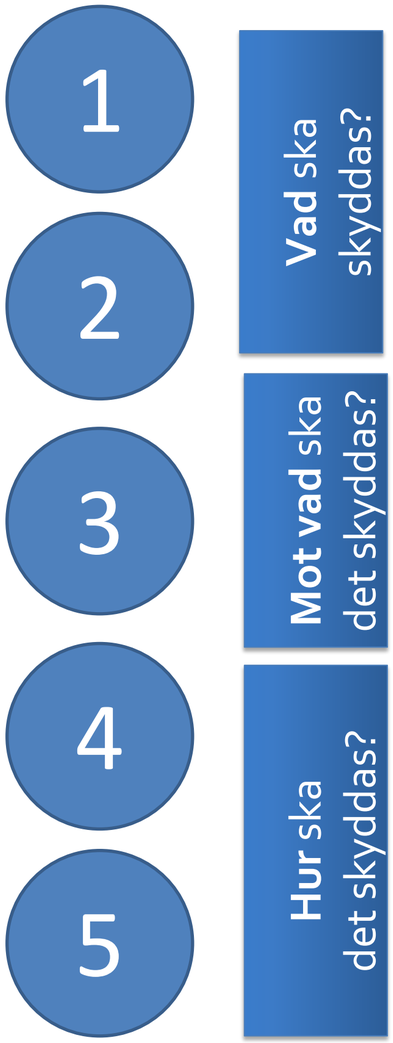
III Beskriv varför en verksamhet bedöms som säkerhetskänslig.

IV Identifiera om det hos den säkerhetskänsliga verksamheten finns direkta eller uppenbart indirekta beroenden till andra verksamheter, både internt och externt

0

Källa: Säkerhetspolisen

Säkerhetskyddssanalys - steg för steg



Identifiera och fastställa skyddsvärden

Konsekvensanalys

Fastställa hot och genomföra analys av hot

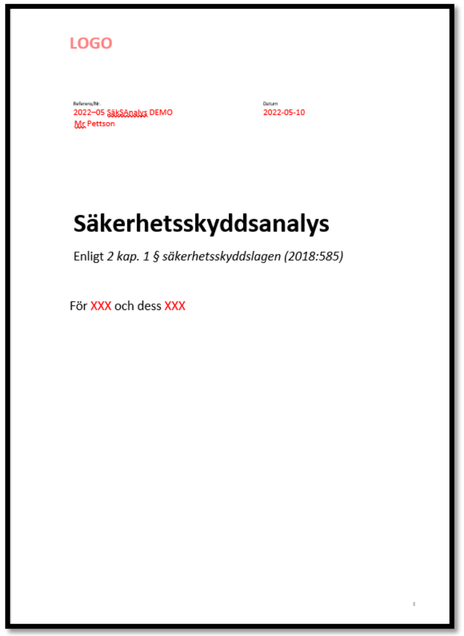
Sårbarhetsanalys

Säkerhetsskyddsåtgärder definieras

Hotanalys

	A	B	C	D	E	F
1	**Skyddvärdena**		**Varför viktigt**	**Varför skyddsvärt**	**Konsekvens**	**H**
2	**Nätinfrastruktur**	**•Fiber till master antingen egen ägd eller hy**	•Skydd, undsättning och vård	Nätstruktur, helhet. Ej en enskilda masten	Bristande tillgänglighet	Fysisk åt
3		**•Radiolänk hopp mera sällan**	* 112		Bristande tillgänglighet	Fysisk/logisk åtkomst fö
4		**•Lätt åtkomst i fiberbrunnar**	•Polisen personskydd		Kan slå ut hel station med enkla medel	Fysisk åtkomst för sabotage eller spion
5		**• Nätdokumentation**	* Positionering		Identifiera svaga punkter och kartläggning	Kartläggning inför sabotage
6			* Ekonomiska transaktioner			
7	**Site master**	**•Sammarbetscluster**	•Krisledning		Identifiera svaga punkter och kartläggning	Kartläggning inför sabotage eller spionage
8		**Basstationer**	* Företag och myndigheters informationsdelning	Begränsa riktakte attacker	Bristande tillgänglighet alt ingen tillgänglighet	Fysisk åtkomst för sabotage och spionage, inplacering av falsk utrustning, störa
9		**Siter**		Begränsa riktakte attacker	Bristande tillgänglighet	Fysisk åtkomst för sabotage och spionage, inplacering av falsk utrustning
10		**•Datorhallar**			Informationläkage, bristande tillgänglighet	Fysisk åtkomst för sabotage och spionage, inplacering av falsk utrustning
11						
12	**Tjänster**	Taltjänster			Oro och bristande ledningsförmåga avlyssning	Logisk åtkomst för blockering och avlyssning
13		IP-baserade tjänster		Allt bygger på internet	Bristande ledningsförmåga, oro brist på tillgänglighet	Logiska attacker, blockering, ex Ddos-attacker och avlyssning, mot nätet
14		**•Telematiktjänster IoT**		Ofta kritiska tjänster	Bristande ledningsförmåga, oro brist på tillgänglighet	Logiska attacker, blockering, ex Ddos-attacker och avlyssning, mot nätet
15		**•Positioneringstjänster**			Bristande ledningsförmåga, oro brist på tillgänglighet, personhot	Logiska attacker, blockering, ex Ddos-attacker och avlyssning, mot nätet
16		**Larmtjänster överföring**			Bristande ledningsförmåga, oro brist på tillgänglighet, brottslig förberedelse/genomförande	Logiska attacker, blockering, ex Ddos-attacker och avlyssning, mot nätet
17		Nätlogik		Central nätfunktionalitet	Bristande ledningsförmåga, oro brist på tillgänglighet, brottslig förberedelse/genomförande	Logisk åtkomst för sabotage eller spionage
18						
19	**Personal**	Nätadministratörer		Åtkomst till skyddsvärd information/anläggningar	Antagonist får tillgång till information, Bristande tillgänglighet	Åtkomst till information för sabotage eller spionage
20		NOC personal		Åtkomst till skyddsvärd information/anläggningar	Antagonist får tillgång till information, Bristande tillgänglighet	Åtkomst till information för sabotage eller spionage
21		Nätplanerare		Åtkomst till skyddsvärd information/anläggningar	Antagonist får tillgång till information	Åtkomst till information för sabotage eller spionage
22		IT-administratörer		Åtkomst till skyddsvärd information/anläggningar	Antagonist får tillgång till information	Åtkomst till information för sabotage eller spionage
23		Väktare och säkerhetspersonal		Åtkomst till skyddsvärd information/anläggningar	Antagonist får tillgång till information, underlättar för intrång och sabotage	Fysisk åtkomst för sabotage och spionage
24						
25						
26	Proces					
27						
28						
29						
30						
31						
32	Dokum					
33						
34						

	A	B	F	G	H	I	J
1	**Skyddvärdena**		**Hot**	**Hotskala 1-4**	**Hotaktör**	**Sårbarhet**	**Skyddsåtgärder**
2	**Nätinfrastruktur**	**•Fiber till master antingen egen ägd eller hy**	Fysisk åtkomst för sabotage eller spionage	3	Främmande makt,	Följer ej branchens anvisningar för Robust fiber	Besiktningar och revision internt.
3		**•Radiolänk hopp mera sällan**	Fysisk/logisk åtkomst för sabotage eller spionage, störa mobilradio frekvenser	1	Främmande makt,	Placerad på tillgänglig höjd	Kravställd moteringsanvisning som skall följas
4		**•Lätt åtkomst i fiberbrunnar**	Fysisk åtkomst för sabotage eller spionage	3	Främmande makt,	Ej nergrävda och ej låsta	Gräv ner och lås!!!
5		**• Nätdokumentation**	Kartläggning inför sabotage	4	Främmande makt	Bristfällig behörighetssystem	Kravställa mot systemleverantörer på behörighetshantering
6							
7	**Site master**	**•Sammarbetscluster**	Kartläggning inför sabotage eller spionage	3	Främmande makt	Brister i avtal för sammarbete och information	Säkerställ avtalshantering
8		**Basstationer**	Fysisk åtkomst för sabotage och spionage, inplacering av falsk utrustning, störa	2	Främmande makt,	Frilliggande kablage mellan mast och basstation	Fysiskt åtkomst skydd
9		**Siter**	Fysisk åtkomst för sabotage och spionage, inplacering av falsk utrustning	3	Främmande makt,	Många entreprenörer	Sektionera siterna
10		**•Datorhallar**	Fysisk åtkomst för sabotage och spionage, inplacering av falsk utrustning	4	Främmande makt	Hög koncentration av kritisk utrustning	Sprid riskerna
11							
12	**Tjänster**	Taltjänster	Logisk åtkomst för blockering och avlyssning	3	Främmande makt,	Bristfällig kryptering	ingen åtgärd finns kompletterande tjänster
13		IP-baserade tjänster	Logiska attacker, blockering, ex Ddos-attacker och avlyssning, mot nätet	3	Främmande makt,	Internets öppenhet	tekniska skyddsåtgärder
14		**•Telematiktjänster IoT**	Logiska attacker, blockering, ex Ddos-attacker och avlyssning, mot nätet	3	Främmande makt,	Internets öppenhet	Ökad it-säkerhets kunskap,
15		**•Positioneringstjänster**	Logiska attacker, blockering, ex Ddos-attacker och avlyssning, mot nätet	2	Främmande makt,	Otillräcklig kunskap och regelverk	Förtydliga regelverket med tillhörande utbildning
16		**Larmtjänster överföring**	Logiska attacker, blockering, ex Ddos-attacker och avlyssning, mot nätet	3	Främmande makt,	inte sekretessavtal med larmoperatör	Rätt avtal motsvarande SUA
17		Nätlogik	Logisk åtkomst för sabotage eller spionage	4	Främmande makt,	Hög koncentration av kritisk information	Säkerhetsprövad all berörd personal
18							
19	**Personal**	Nätadministratörer	Åtkomst till information för sabotage eller spionage	4	Främmande makt,	Outsourcad personal	Revision av outsourcing bolaget.
20		NOC personal	Åtkomst till information för sabotage eller spionage	4	Främmande makt,	Inte säkerhetsprövad personal	Säkerhetsprövad personal
21		Nätplanerare	Åtkomst till information för sabotage eller spionage	4	Främmande makt,	Insiderproblematik	Kontinuerliga säkerhetssamtal
22		IT-administratörer	Åtkomst till information för sabotage eller spionage	4	Främmande makt,	Hög behörighet	Strikt behörighetspolicy som skall efterlevas
23		Väktare och säkerhetspersonal	Fysisk åtkomst för sabotage och spionage	1	Främmande makt,	Stor omsättning av personal	Loggning och uppföljning
24		Service underhållspersonal	Fysisk åtkomst för sabotage och spionage	2	Främmande makt,	Utnyttjas av många operatörer ändlig resurs, Agregerad informationskunskap	Begränsa informationsspridning
25							
26	**Processer**	**Krishantering, t ex flytt till reservplats**	Kartläggning inför sabotage eller spionage	2	Främmande makt	Brister i informationssäkerhet	Begränsa tillgång till enbart behövande
27		**Felavhjälpning**	Kartläggning inför sabotage eller spionage	1	Främmande makt (	Öppen information på interna nät	Minimera den publika informationens detaljrikedom
28		**Avbrottshantering**	Kartläggning inför sabotage eller spionage	1	Främmande makt (	Öppen information på interna nät	Minimera den publika informationens detaljrikedom
29		**Upphandling**	Säkerhetskrav beaktas ej får in främmande spioner i organisationen	2	Främmande makt (	Brister i upphandligsunderlagen	Ta med säkerhetsskyddet vid upphandling
30		**Avveckling**	Känslig information lämnas kvar vid avveckling	2	Främmande makt	Brist på rutiner och uppföjning	Tydliga rutiner för informationssäkerhet och kontroller
31							
32	**Dokument**	**Säkerhet/sårbarhetsanalyser**	Kartläggning inför sabotage eller spionage	3	Främmande makt (	Förvaras felaktigt	Förvara i godkända säkerhetsskåp
33		Tillträdesskyddet	Kartläggning inför sabotage eller spionage	2	Främmande makt,	Öppenhet i tekniska lösningen	Anonyma kort
34							



LOGO

Referens/Nr
2022-05 SäkSåanalys DEMO
Mc Pettson

Datum
2022-05-10

Säkerhetsskyddsanalys

Enligt *2 kap. 1 § säkerhetsskyddslagen (2018:585)*

För XXX och dess XXX

Säkerhetsskydds-analys

Innehållsförteckning

1 Allmänt 4
2 Inledning 4
3 Beslut att fastställa säkerhetsskyddsanalysen 4
4 Beslut om inplacering i säkerhetsklass 4
5 Säkerhetsskyddschef 4
6 Verksamhetsbeskrivning 5
6.1 Bolagets uppdrag enligt ägardirektiv 5
6.1.1 Samhällsviktig Verksamhet 5
6.2 En del av totalförsvaret och av nationellt intresse 5
6.2.1 Föreningen och bolagets betydelse för totalförsvaret 5
6.2.2 Digital infrastruktur, ett nationellt intresse 6
6.2.3 Stadsnätens roll och betydelse ur ett samhällsperspektiv 6
6.2.4 Riksintresse för anläggningar för bredbandsinfrastruktur 6
6.3 Näringslivets verksamheter 6
7 Metodik för identifiering och värdering 7
7.1 Identifiera skyddsvärden och perspektiv 7
7.2 Konsekvenskategorier 7
7.3 Konsekvensnivåer 8
7.4 Säkerhetsskyddsklasser 8
8 Identifiering av säkerhetsskyddsklassificerade uppgifter 9
9 Identifiering av säkerhetskänslig verksamhet 10
9.1 Inplacering i konsekvenskategori och konsekvensnivå 10
9.2 Identifiering av skyddsvärda objekt 11
9.3 Identifiering av informationssystem 12
9.3.1 Informationssystem innehållande säkerhetsskyddsklassade uppgifter 12
9.3.2 Informationssystem med betydelse för säkerhetskänslig verksamhet 12
9.3.3 Identifiering av personal 13
10 Säkerhetshot 14
10.1 Främmande makt 14
10.2 Terrorism 15
10.3 Organiserad brottslighet 15
10.4 IT-angrepp 15
10.5 Icke antagonistiska hot 15
10.6 Sammanfattning 15
11 Sårbarhetsbedömning 16
12 Säkerhetsskyddsåtgärder 16
12.1 Informationssäkerhet 16
12.2 Fysisk säkerhet 16
12.3 Personalsäkerhet 17
12.4 Rutin för säkerhetsskydd 17
13 Sammanställning och beslut 17
Bilaga 1 Referenser 18

Ändringar i Säkerhetsskyddslagen den 1 december 2021

ÄNDRINGAR

Säkerhetsskyddslagen

- ❑ Anmälan om säkerhetskänslig verksamhet
- ❑ Säkerhetsskyddschefens roll
- ❑ Säkerhetsskyddsavtal
- ❑ Särskild säkerhetsskyddsbedömning och lämplighetsprövning
- ❑ Tillsyn, vitesföreläggande och sanktionsavgifter

Trädde i kraft den 1 december 2021

TLP:WHITE

Säkerhetsskyddschefens roll

- Säkerhetsskyddschefens organisatoriska placering
  - Direkt underställd ledningen
    - Ej tillräckligt med rapporteringskrav
    - Typiskt sett ingå i ledningsgrupp/organisatorisk del av ledningen
    - Ska ha en reell möjlighet att ge stöd åt och påverka ledningen i frågor som involverar säkerhetsskyddsaspekter
    - Hindrar inte att säkerhetsskyddsarbetet bedrivs inom flera enheter
    - Fråntar inte ansvar för säkerhetsskydd som åvilar den som är ytterst ansvarig
    - Moder- och dotterbolag ses inte som en enhet

- Säkerhetsskyddsfrågor ska prioriteras

TLP:WHITE

Utökat krav på säkerhetsskyddsavtal 4 kap. 1 § (ny)

1. kvalificerat hemlig vid en synnerligen allvarlig skada,
2. hemlig vid en allvarlig skada,
3. konfidentiell vid en inte obetydlig skada, eller
4. begränsat hemlig vid endast ringa skada.

En verksamhetsutövare som avser att genomföra en **upphandling**, **ingå ett avtal eller inleda en samverkan eller ett samarbete med en annan aktör** ska ingå ett säkerhetsskyddsavtal med aktören, om aktören genom förfarandet kan **få tillgång till**

1. säkerhetsskyddsklassificerade uppgifter i säkerhetsskyddsklassen **konfidentiell eller högre**, eller
2**. annan säkerhetskänslig** verksamhet av motsvarande **betydelse för Sveriges säkerhet**.

Verksamhetsutövaren ska även ingå ett säkerhetsskyddsavtal med en **underleverantör** som anlitas för att fullgöra den andra aktörens förpliktelse, om underleverantören genom sitt uppdrag kan få en sådan tillgång till den säkerhetskänsliga verksamheten som anges i första stycket.

Ett säkerhetsskyddsavtal ska ingås innan motparten kan få tillgång till den säkerhetskänsliga verksamheten.

Sammanfattning
Säkerhet för nätägare

IoT/OT-SÄKERHET

SÄKER FYSISK FÖRBINDELSE

SITE FÖR KRITISK VERKSAMHET

TLP:WHITE

SÄKERHETSARBETE FÖR NÄTÄGARE AV DIGITAL INFRASTRUKTUR

LAGRUM

Driftsäkerhet
IT-säkerhet
Informationssäkerhet

Säkerhetsskydd

Lagen om elektronisk kommunikation **(LEK) 2003:389**
Förordning om elektronisk kommunikation **2003:396**

PTS Driftsäkerhetsföreskrifter
PTSFS 2015:2 och **PTSFS 2020:1**

Offentlighets- och sekretesslagen **(OSL) 2009:400**

Lag (2006:544) om kommuners och regioners åtgärder inför och vid extraordinära händelser i fredstid och höjd beredskap

Lag (1992:1403) om totalförsvar och höjd beredskap

Lag (2018:1174) om informationssäkerhet för samhällsviktiga och digitala tjänster (NIS)

Säkerhetsskyddslagen **2018:585**
Säkerhetsförordning **2021:955**
PMFS 2022:1 Säkerhetspolisens föreskrifter om säkerhetsskydd
PTSFS 2021:2 Post- och telestyrelsens föreskrifter om säkerhetsskydd

Risk- och sårbarhetsanalys På anläggningstillgångar 1

Konsekvensanalys på Verksamhetsdel nätdrift 2

Säkerhetsskyddsanalys 3

VERKTYG

Åtgärder av olika slag
- Direkta åtgärder
- Schemalagda åtgärder
- Periodiska åtgärder
- Förbättringar
- Förstärkningar

Inbjudan till säkerhetsskyddsutbildning:

Praktiskt säkerhetsskyddsarbete för stadsnät

Den 1 december 2021 trädde nya bestämmelser i säkerhetsskyddslagen samt en ny säkerhetsförordning i kraft. De nya bestämmelserna ställer bland annat högre krav på verksamhetsutövare som bedriver säkerhetskänslig verksamhet. För att stadsnäten på ett enklare sätt ska kunna möta dessa nya bestämmelser har Stadsnätsföreningen, tillsammans med SiSG:s säkerhetsråd, tagit fram ett nytt utbildningsprogram för säkerhetsskydd som riktar sig till de som har ett verksamhets- eller säkerhetsansvar, samt de som arbetar praktiskt med säkerhetsfrågor på ett stadsnät.

Med planerad start under april 2022 börjar den första delen i utbildningsprogrammet som består av tre block och sträcker sig över två månader. Första blocket hålls digitalt för att sedan övergå till en kombination av he[illegible] i Stockholm. Hemuppgifterna är anpass[illegible] och som en grund för det fortsatta säke[illegible]

Upplägg

Utbildningsblock 1:
Längd: 1 dag
Fokus: Varför säkerhetsskydd? Hur skapar vi förutsättningar för ett eget lyckat säkerhetsskyddarbete?
Hemuppgift nr. 1

Utbildningsblock 2:
Längd: 2 dagar
Fokus: Praktiskt säkerhetsskyddsarbete. Ledningssystem Säkerhetsskydd.
Hemuppgift nr. 2

Utbildningsblock 3:
Längd: 1 dag
Fokus: Nyheter på området samt avslutning. Sammanfattning och redovisning av lärandet. Inspirationsföreläsning

Utbildningstillfällen

Pågående kurs. Avslutat 14 juni 25 personer

Utbildningstillfälle 1:
5 april – 20 juni 2022

Utbildningstillfälle 2:
7 september – 11 november 2022

Ett fåtal platser kvar. Planerat vår och höst 2023

Observera att datena är preliminära och kan komma att ändras.

https://www.ssnf.org/kurs--konferens/utbildning/

TLP:WHITE

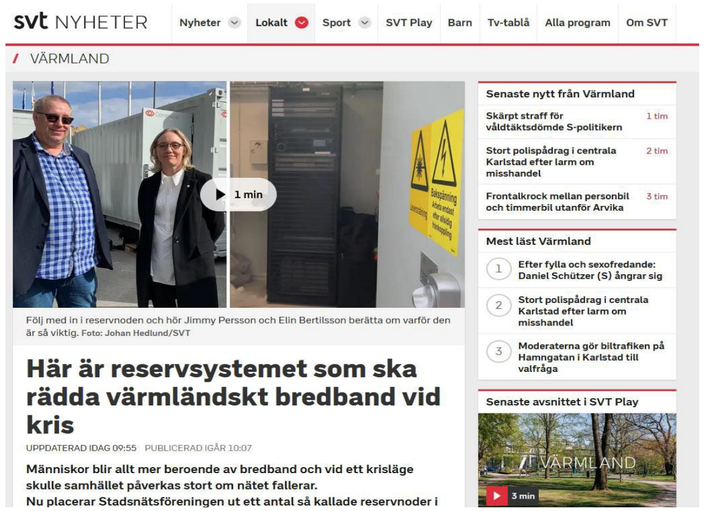
EXEMPEL PÅ EN BEREDSKAPSHÖJANDE ÅTGÄRDER

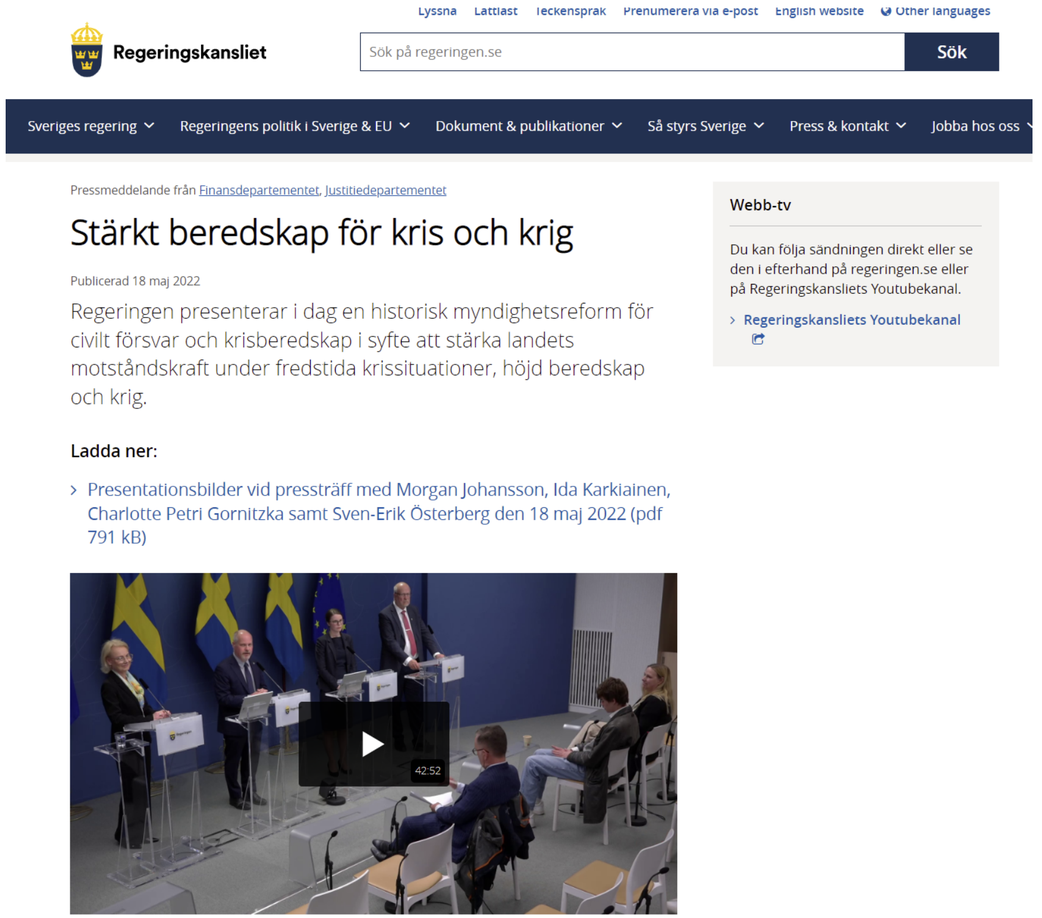
Motståndskraft och uthållighet
Bakgrund

Det förändrade säkerhetspolitiska läget har lagt fokus på försvarsförmågan för Sveriges i fall ett anfall eller ett antagonistiskt hot riktar sig mot Sveriges.

Som en del i försvaret upprustning och förmågeförhöjning så är sektorn **elektronisk kommunikation utpekad som en infrastruktur som ska skyddas vid ett sådant läge**. MSB har fått till uppgift att samordna resursbehovet för uppbyggnad av det civila försvaret, vilket är en del av totalförsvaret.

Det handlar om **att öka förmåga till att bland annat reparera förbindelser och siter**.





Ett starkare Sverige

Satsningar på det civila försvaret och krisberedskapen

Största satsningen i modern tid

- Återuppbyggnad av det civila försvaret
- 4,7 miljarder kr per år
- Ytterligare 800 miljoner kronor under 2022
- Ytterligare insatser 2023-2025

Stärkt motståndskraft

Största myndighetsreformen för civilt försvar och krisberedskap

- 60 beredskapsmyndigheter
- 10 beredskapssektorer
- 10 sektorsansvariga myndigheter
- 6 civilområden
- 6 civilområdesansvariga länsstyrelser

10 beredskapssektorer och sektorsansvariga myndigheter

Hälsa, vård och omsorg	Livsmedelsförsörjning och dricksvatten	Ordning och säkerhet	Räddningstjänst och skydd av civilbefolkningen	Transporter
Socialstyrelsen	Livsmedelsverket	Polismyndigheten	Myndigheten för samhällsskydd och beredskap	Trafikverket

Ekonomisk säkerhet	Elektroniska kommunikationer och post	Energiförsörjning	Finansiella tjänster	Försörjning av grunddata
Försäkringskassan	Post- och telestyrelsen	Energimyndigheten	Finansinspektionen	Skatteverket

Robust Reservnod

- Robust reservnod. Vad är det?

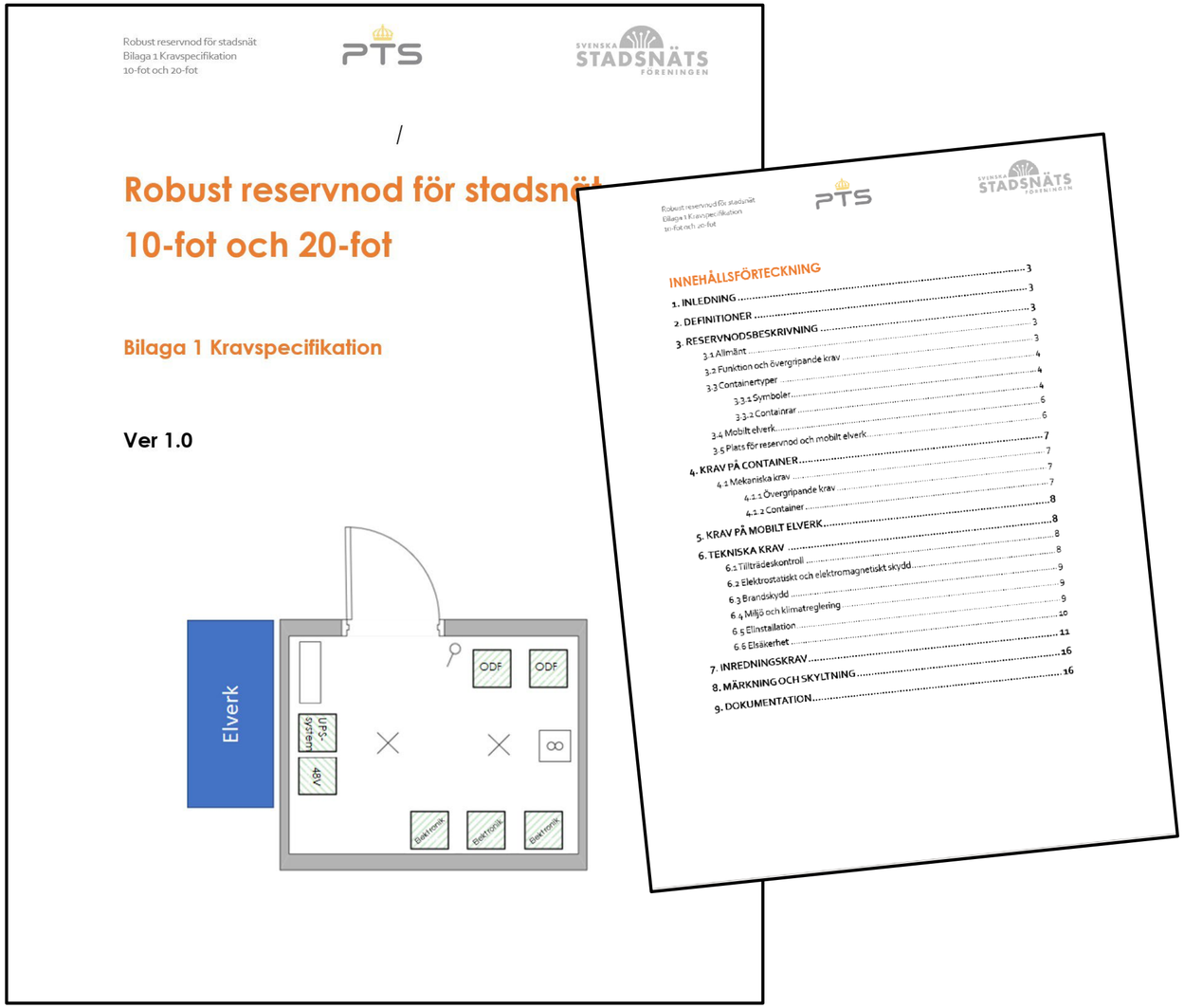
- Användningsområden

- Teknisk data / Faktablad

- Nodberedskap

Coromatic

Robust Reservnod för Stadsnät



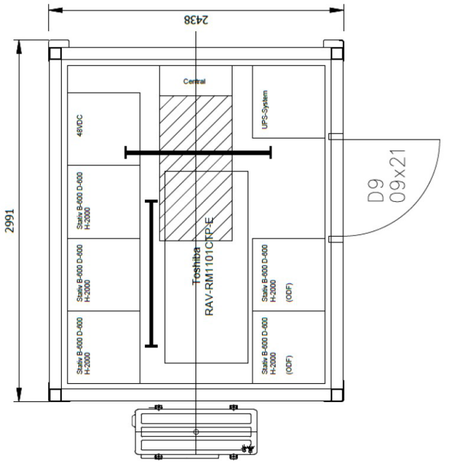
Robust Reservnod för Stadsnät: Användningsområden

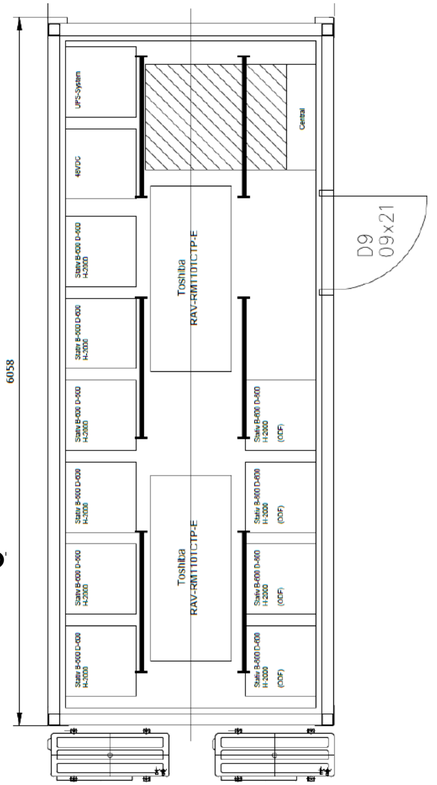
FAKTABLAD

Förstärkningsresursen omfattar en containerlösning med följande omfattning:

- 1 st Container typ1 (10-fot)
- 1 st Container typ2 (20-fot)
- 2 st Mobila elverk med extra bränsletankar

Förstärkningsresursen ska kunna ersätta en skadad ordinarie fast nätnod alternativt utgöra ett komplement vid behov av förstärkning eller förändring av ordinarie nod.

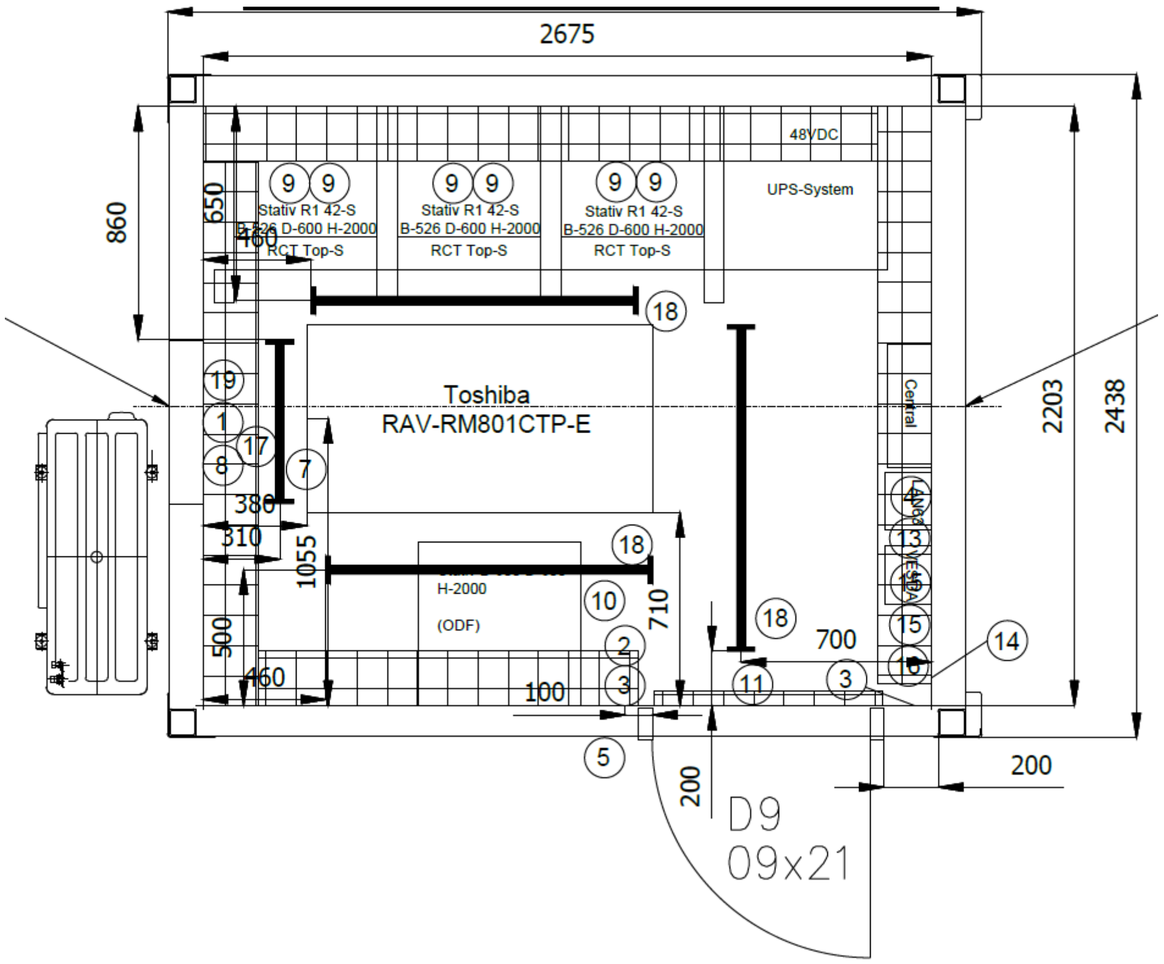




Funktion och övergripande krav

- Reservnoden kan **hantera olika kapacitetsbehov genom dockning** av flera passiva nodcontainrar.
- Containrarna är **mobila och kan transporteras med lastbil till reservplats**. Reservplats ska vara förberedd.
- Containrarna är **väderisolerade och utrustade med värme och frikyla**.
- Containrarna är försedda **med dörr och nyckelsystem samt passagekontrollsystem** med kod alternativt tag.
- Containrarna har egen **elcentral och primärt strömförsörjs från det allmänna elnätet** via ett externt 3-fasintag, och sekundärt från ett externt mobilt elverk.
- Containrarna är inredda **med stativ för ODF-enheter och rack för installation av aktiv utrustning, skåp för 48V strömförsörjning och avbro**
- Containrarna innehåller **anslutningskablar i olika dimensioner**.
- Containrarna innehåller **patchkablar i olika dimensioner**.
- Containrarna har uttag för **jordtag med jordspett.**

Reservnod förmåga: 10-fot container



Container typ 1

FAKTABLAD

Egenskap	Tekniska data
Storlek	Teknikmodul bestående av 10 fots ISO container.
Vikt	4000kg
Transport	Lastbil/Lastväxlare
Normal inställelsetid	Enligt överenskommelse

Container Typ 1 (10 fot)

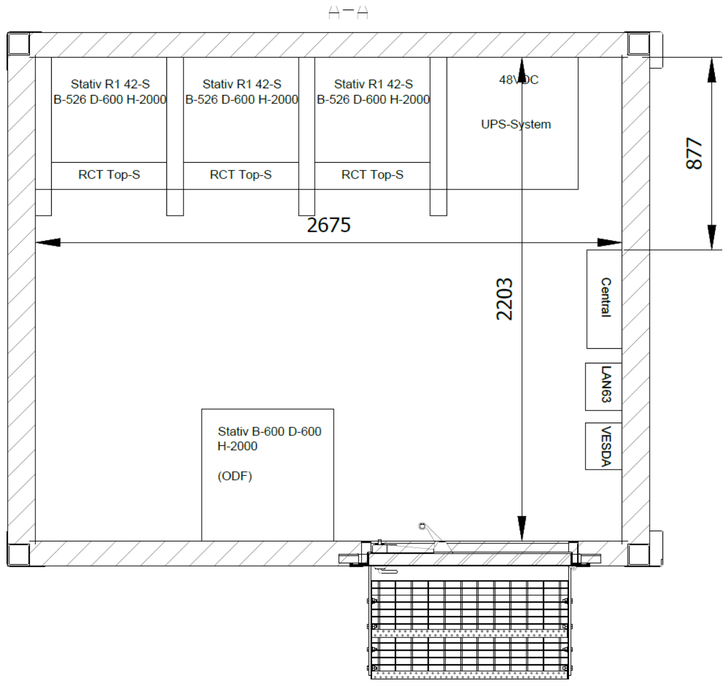
- Yttermått: L: 2991mm, B: 2438 mm, H: 2591 mm
- Innermått: L: 2831 mm, B: 2377 mm, H: 2376 mm, Volym: 15.98 kbm Yta: 6,7kvm

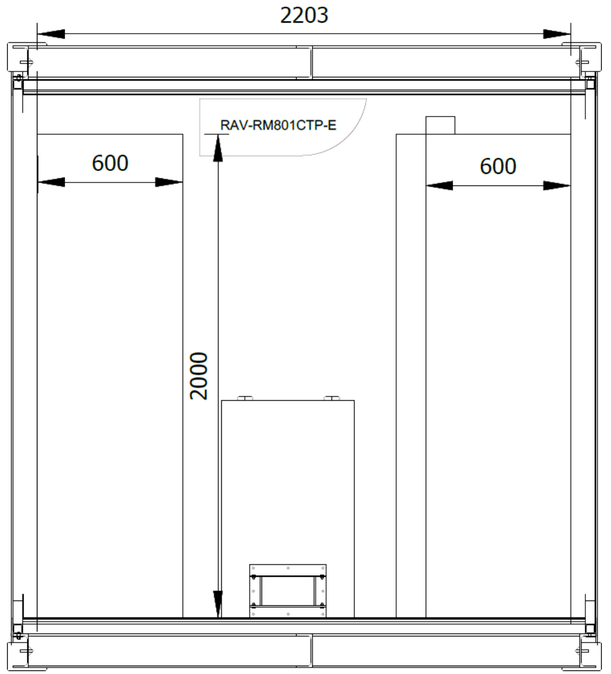
126 HE i kapacitet

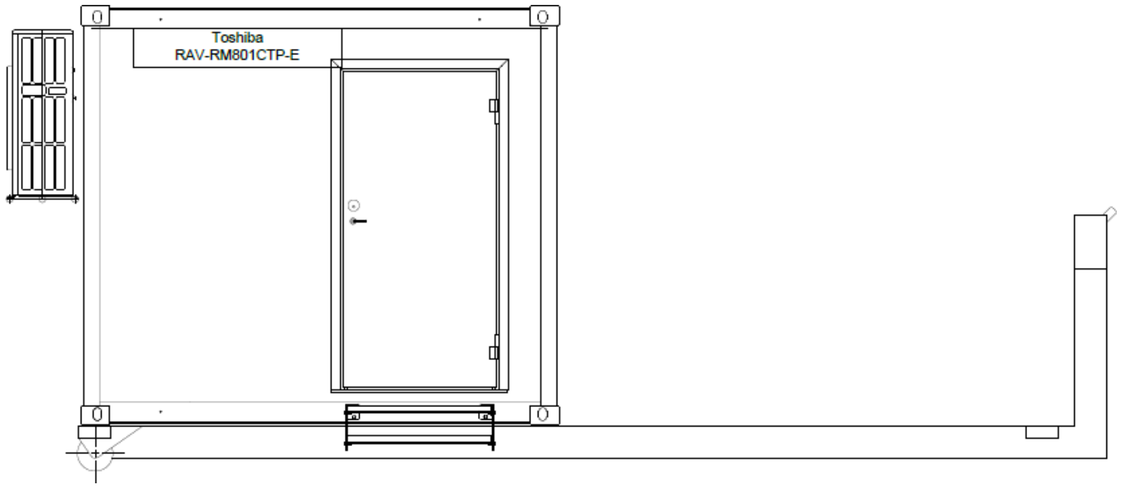
Container typ 1

FAKTABLAD

Egenskap	Tekniska data
Elsystem	Automatisk växling mellan nätkraft och reservkraft. System för avbrottsfri kraft. Likriktare (n+1, 6 kW i kontinuerlig drift) och distributionscentral för 48V, Växelriktare (n+1, 1000VA kontinuerlig drift) och distributionscentral för 230V avbrottsfri kraft
Gränssnitt	48VDC resp. 230VAC
System för miljö och klimatreglering	Kylaggregat 1st TOSHIBA SDI. Kyleffekt 12kW.
ODF	2 stativ / 6 ODF-enheter (B 526, D 600, H 2000/42HE)
Elektronikstativ	3 stativ (B 526, D 600, H 2000/42 HE)
Inbrottsskydd	Klass 3
Brandskydd	Brandteknisk klass EI30.
Övervakning	Larmpanel typ LAN63. - Hög rumstemperatur - Larm kylaggregat - Larm 48VDC/UPS - Larm luftfuktighet (RH) - Brandlarm (från detekteringssystem Vesda VLF-250) - Summalarm A reservkraft - Summalarm B reservkraft - Driftindikering reservkraft
Passagekontrollsystem	Entrédörr med passagekontrollssystem (standalone) med RCO kortläsare för tag, dag- och nattlåsning med elslutbleck samt motorlås typ ASSA 840C-50 Hi-O.
Kabelintag fiber	Lucka för genomföring för fiber med Roxtec S6x1 genomföring
Kabelintag el	Lucka för genomföring för kraftmatning med Roxtec S6x1 genomföring

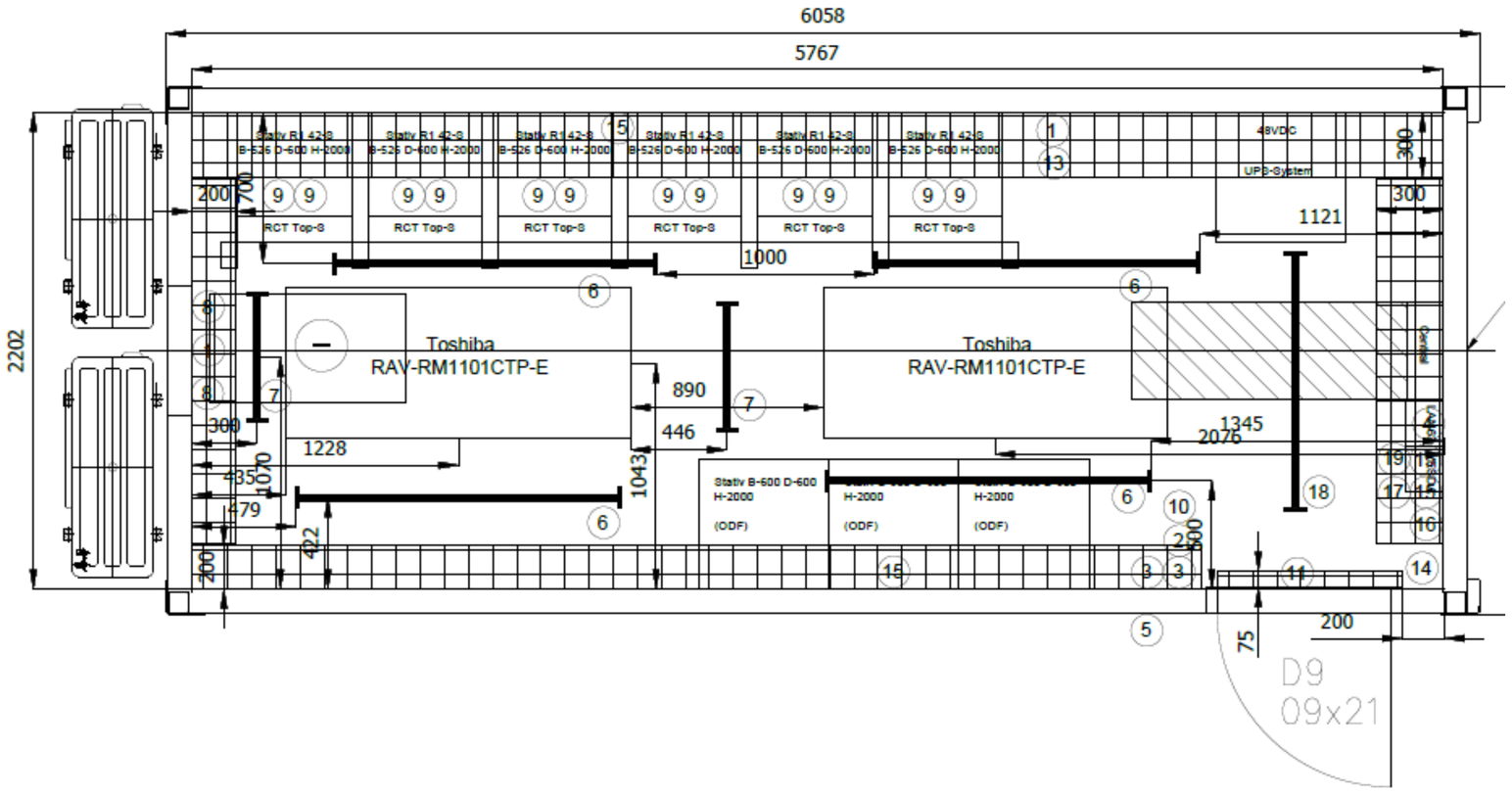






TLP:AMBER

Reservnod förmåga: 20-fot container



Container 2

FAKTABLAD

Egenskap	Tekniska data
Storlek	Teknikmodul bestående av 20 fots ISO container.
Vikt	6300kg
Transport	Lastbil/Lastväxlare
Normal inställelsetid	Enligt överenskommelse

Mått

Container Typ 2 (20 fot)

- Yttermått: L: 6058 mm, B: 2438 mm, H: 2591 mm (ISO standard)
- Innermått L: 5898 mm, B: 2350 mm, H: 2390 mm, Volym: 33.1 kbm Yta: 13.8kvm

252 HE i kapacitet

Reservnod förmåga: Kablage och stativ

Container typ 1

FAKTABLAD

Egenskap	Tekniska data
Anslutningskablar	4 st 100m 96 fiberkabel SM G. 657A1 1 st 100m 192 fiberkabel SM G. 657A1 1 st 100m 384 fiberkabel SM G. 657A1
Dockningskablar	1 st fiberoptisk dockningskabel, 96 fiberkabel SM G. 657A1. Kabellängd 50m.
Patchkablar	200 st 10m singel patchkabel SM G. 657A1 300 st 7m singel patchkabel SM G. 657A1 400 st 5m singel patchkabel SM G. 657A1
Skarvboxar	5 st skarvboxar för fiberskarvning av anslutningskablar till externt nät.

Container typ 2

FAKTABLAD

Egenskap	Tekniska data
Anslutningskablar	4 st 100m 96 fiberkabel SM G. 657A1 4 st 100m 192 fiberkabel SM G. 657A1 2 st 384 fiberkabel SM G. 657A1
Dockningskablar	1 st fiberoptisk dockningskabel, 96 fiberkabel SM G. 657A1. Kabellängd 50m.
Patchkablar	400 st 10m singel patchkabel SM G. 657A1 600 st 7m singel patchkabel SM G. 657A1 800 st 5m singel patchkabel SM G. 657A1
Skarvboxar	10 skarvboxar för fiberskarvning av ovanstående kablar till externt nät.

Container typ 1

FAKTABLAD

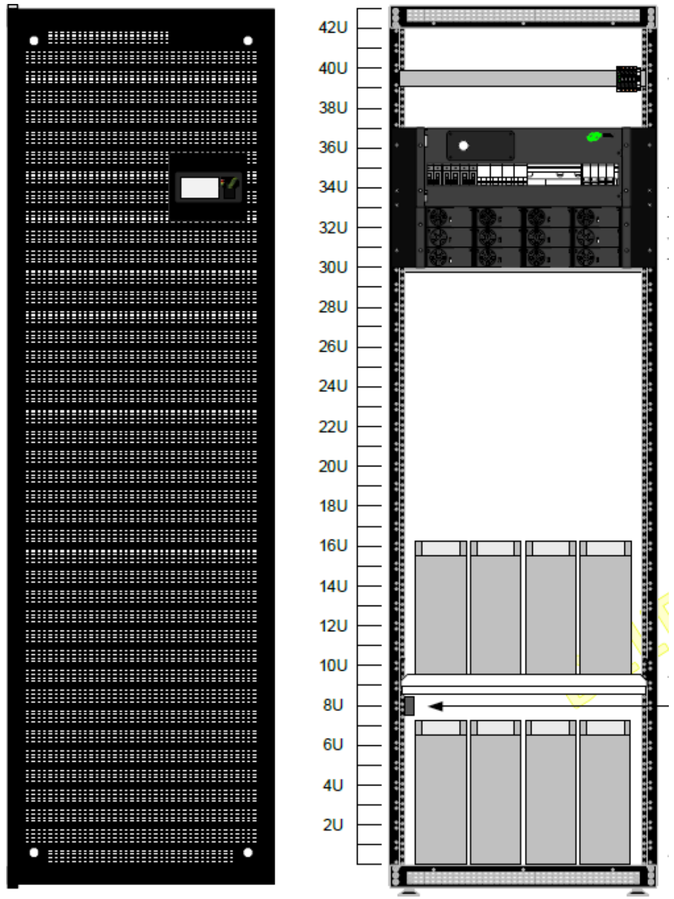
Egenskap	Tekniska data
Elektronikstativ	3 stativ (B 526, D 600, H 2000/42 HE)

Container typ 2

FAKTABLAD

Egenskap	Tekniska data
Elektronikstativ	6 stativ (B 526, D 600, H 2000/42 HE)

378 HE i kapacitet



Kabelrangering och Kraftdistribution:

Aktiva stativ
- 4-post stativ
- Vertikal/Horisontal kabelrangering

PDUer
- Vertikal PDU 230VAC C13/C19
- Horisontal PDU 48VDC

UPS
- Rectiverter 48VDC/230VAC
- Power moduler Hot-swop

EPI G2

EPI G2 is a range of PDU: s that can
be used alone as reliable power distribution unit without
any monitoring functionality. The PDU can be fitted with a monitoring module
(EPI MM G2) for local and remote monitoring through TCP/IP or ampere module
(EPI AM G2) for local ampere reading.

Container: 1 st 20-fot samt st 10-fot

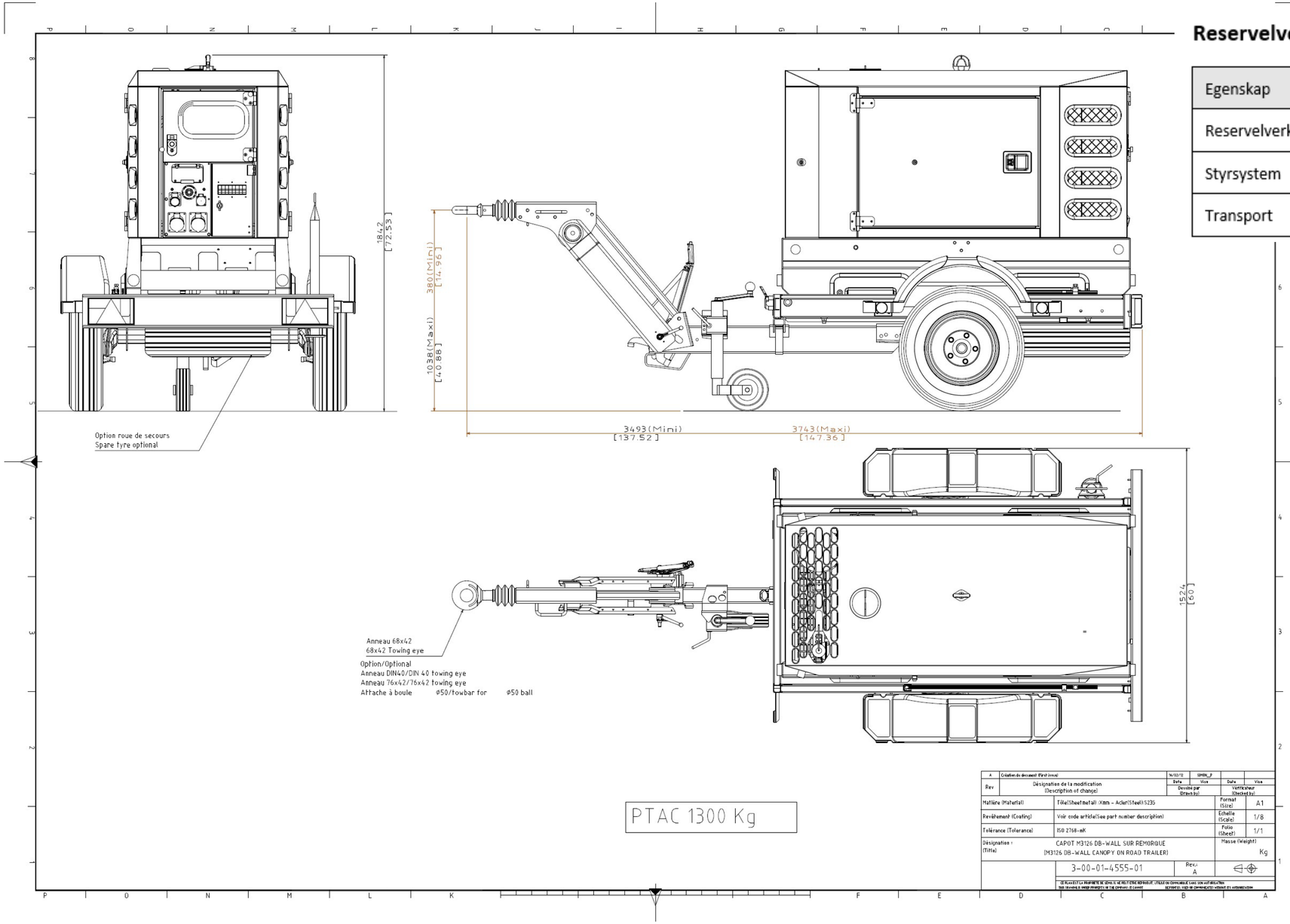
Container: 1 st 20-fot samt st 10-fot

TLP:AMBER

Container: 1 st 20-fot samt st 10-fot

Container: 1 st 20-fot samt st 10-fot

Reservnod förmåga: Reservelverk 20kVA

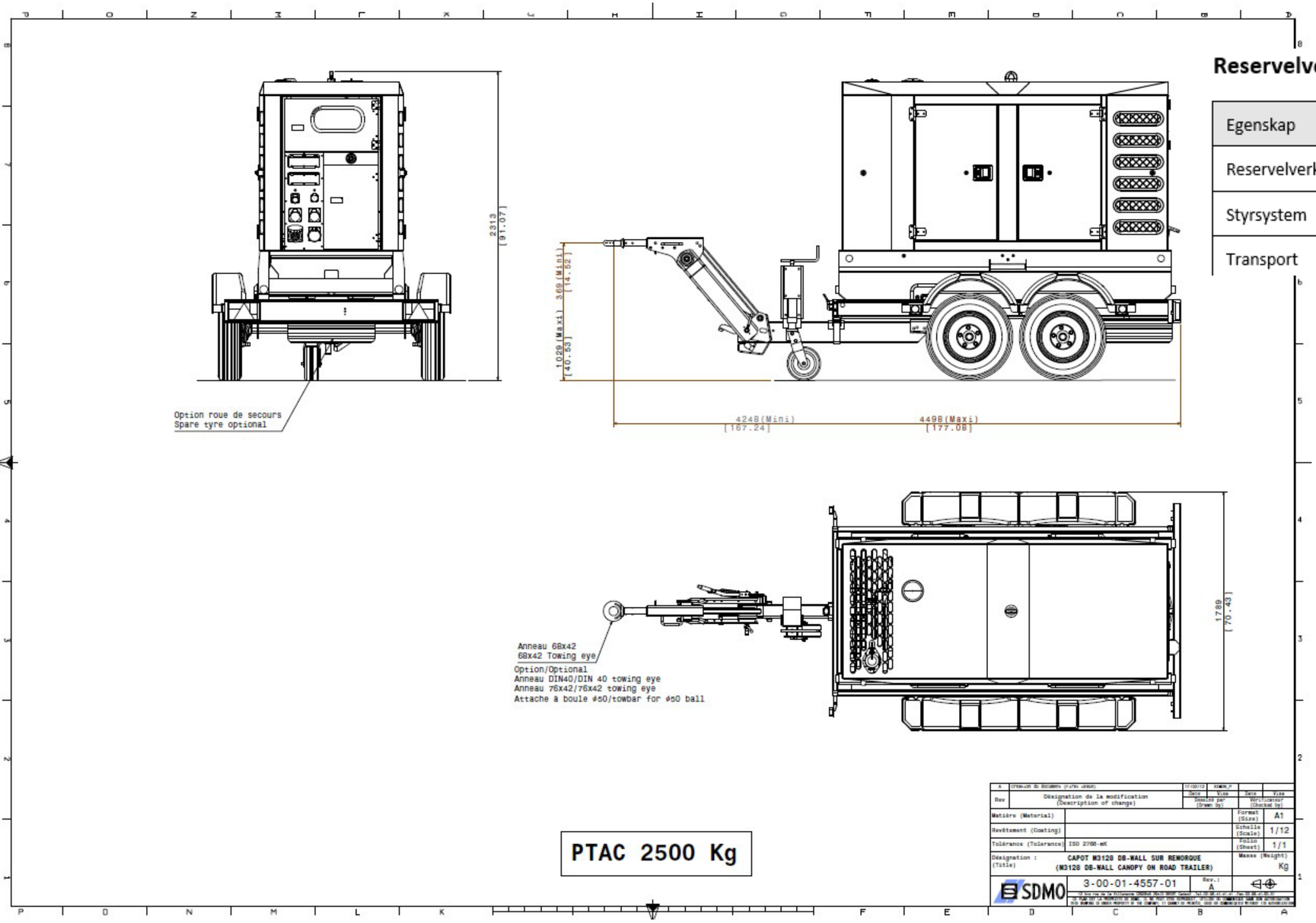


Reservelverk typ 1

FAKTABLAD

Egenskap	Tekniska data
Reservelverk Kohler R20C5	PRP effekt: 18,2 kVA.
Styrsystem	APM403S med fjärrövervakning
Transport	Dragögla.

Reservnod förmåga: Reservelverk: 50kVA

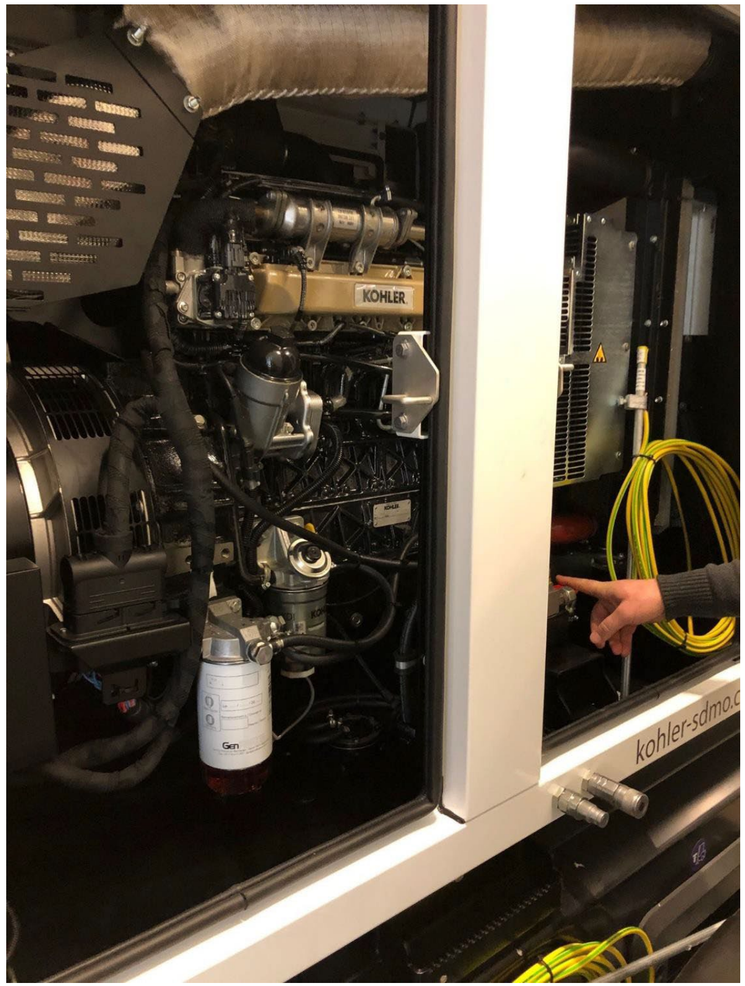


Reservelverk typ 2

FAKTABLAD

Egenskap	Tekniska data
Reservelverk Kohler R50C5	PRP effekt: 45 kVA.
Styrsystem	APM403S med fjärrövervakning
Transport	Dragögla.

Reservnod förmåga: Elverk: 1 st 20kVA + 1 st 50kVA

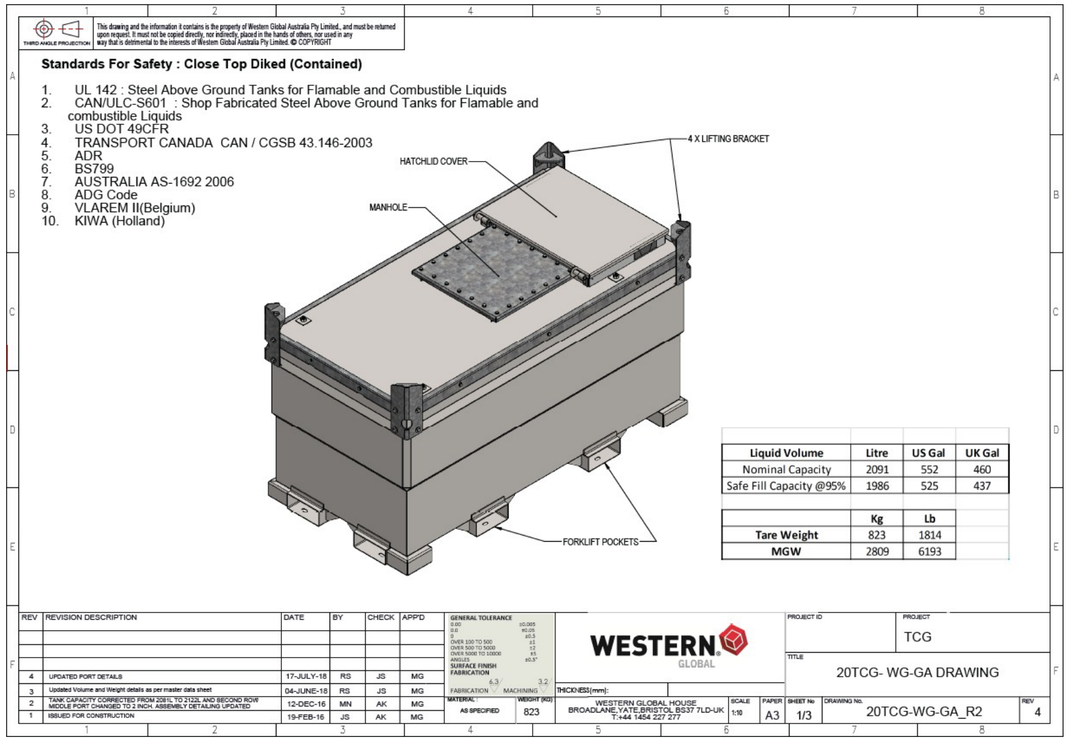


Reservnod förmåga: Bränsletank 10 dygns drift

Extra bränsletank typ 1

FAKTABLAD

Egenskap	Tekniska data	Kommentar
Dubbelmantlad fristående 2000 liters bränsletank	Överfyllnadsskydd och kopplingar/rör för påfyllning/avluftning Erforderliga kranar och ventiler samt 5 m slang mellan motor och tank Givare för larm vid låg bränslenivå Givare för larm vid läckage Potentialfria kontakter/summalarm till plint i styrpanel	Dimensionerad för mer än 10 dygns drift vid 100% last.



Reservnod förmåga:
Bränsletankar för 10 dygns drift. 2000l samt 3000l

Beredskapsansansvariga stadsnät inom SiSG


Rutin för tillhandahållande av Reservnoder för stadsnät

SVENSKA STADSNÄTSFÖRENINGEN

Rutin för tillhandahållande av Reservnoder för stadsnät

Version 0.0

2021-11-11

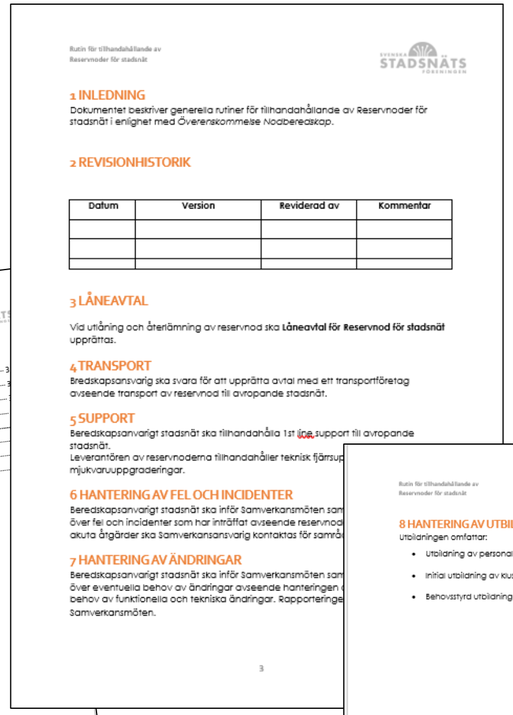
1

Rutin för tillhandahållande av Reservnoder för stadsnät

Innehåll

1 INLEDNING
2 REVISIONHISTORIK
3 LÅNEAVTAL
4 TRANSPORT
5 SUPPORT
6 HANTERING AV FEL OCH INCIDENTER
7 HANTERING AV ÄNDRINGAR
8 HANTERING AV UTBILDNING OCH ÖVNING

2


Rutin för tillhandahållande av Reservnoder för stadsnät

SVENSKA STADSNÄTSFÖRENINGEN

1 INLEDNING

Dokumentet beskriver generella rutiner för tillhandahållande av Reservnoder för stadsnät i enlighet med Överenskommelse Nodberedskap.

2 REVISIONHISTORIK

Datum	Version	Reviderad av	Kommentar

3 LÅNEAVTAL

Vid utlåning och återlämning av reservnod ska **Låneavtal för Reservnod för stadsnät** upprättas.

4 TRANSPORT

Bredskapsansvarig ska svara för att upprätta avtal med ett transportföretag avseende transport av reservnod till avropande stadsnät.

5 SUPPORT

Beredskapsansvarigt stadsnät ska tillhandahålla 1st line support till avropande stadsnät.
Leverantören av reservnoderna tillhandahåller teknisk fjärrsup
mjukvaruuppgraderingar.

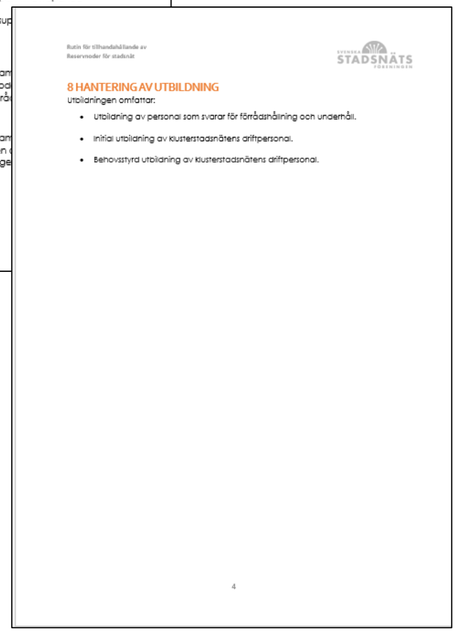
6 HANTERING AV FEL OCH INCIDENTER

Beredskapsansvarigt stadsnät ska inför Samverkansmöten sam
Över fel och incidenter som har inträffat avseende reservnod
akuta åtgärder ska Samverkansansvarig kontaktas för samrå

7 HANTERING AV ÄNDRINGAR

Beredskapsansvarigt stadsnät ska inför Samverkansmöten sam
över eventuella behov av ändringar avseende hanteringen
behov av funktionella och tekniska ändringar. Rapporteringe
Samverkansmöten.

3


Rutin för tillhandahållande av Reservnoder för stadsnät

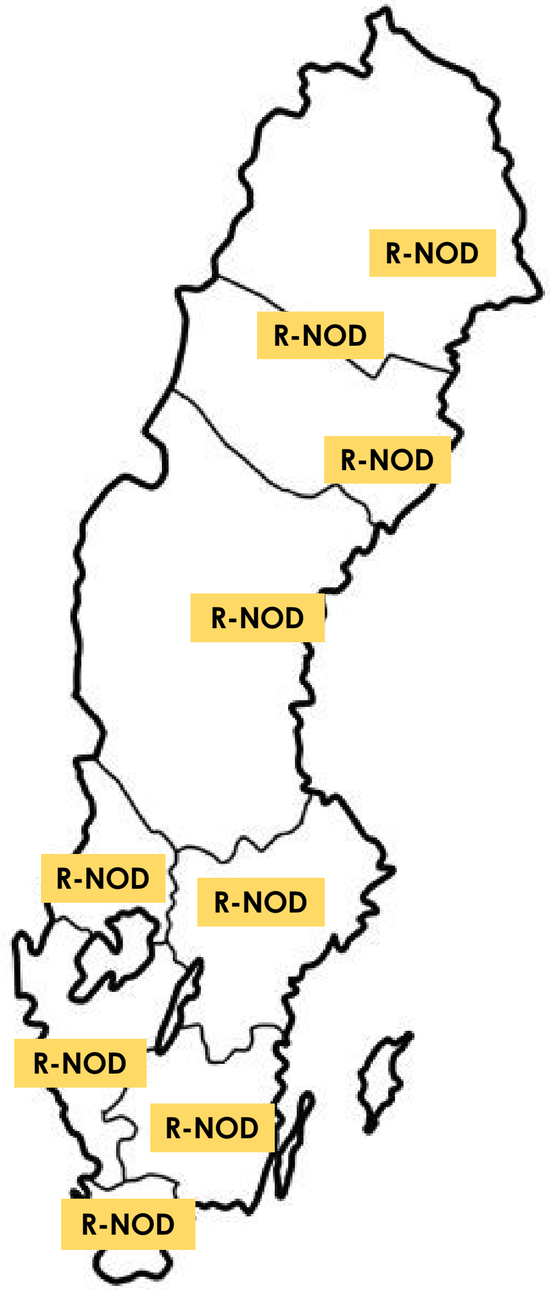
SVENSKA STADSNÄTSFÖRENINGEN

8 HANTERING AV UTBILDNING

Utbildningen omfattar:

- Utbildning av personal som svarar för förråsnåining och underhåll.
- Initial utbildning av klusterstadsnätens driftpersonal.
- Behovsstyrd utbildning av klusterstadsnätens driftpersonal.

4




Coromatic
STAGE
Coromatic
Coromatic

Tack så mycket för att du tittat och lyssnat. Frågor?

Jimmy Persson
Utveckling- och Säkerhetschef
Jimmy.persson@ssnf.org
08-214 640

TLP:WHITE