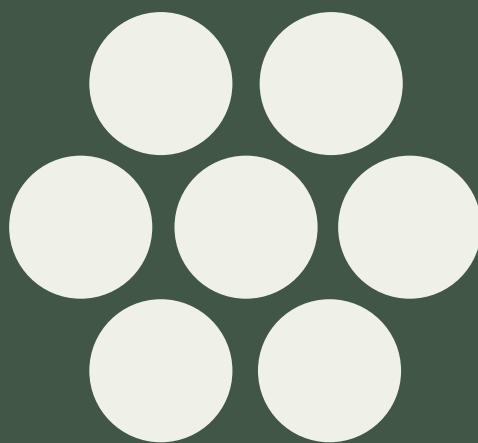


# Anläggningar med förhöjd säkerhet och funktion

Amendments - Rättelser och tillägg

2024-03-01





**Anläggningar med  
förhöjd säkerhet**

## Revisionshistorik:

Datum	Version	Reviderad av	Kommentar
2024-03-01	1.1	Lars Björkman	Revidering i samband med framtagning av kurs
2023-05-01	1.0	Lars Björkman	Införande av Anvisning för anläggningar med förhöjd säkerhet och funktion

## Gällande version för respektive dokument:

Bilaga	Gällande version	Ändrad datum
Huvuddokument	V1.1	
Bilaga 1. Robust site för samhällsviktig digital infrastruktur	V1.1	
Bilaga 1.1 Checklista för Site med förhöjd säkerhet	V1.1	
Bilaga 2. Passiv säker fysisk förbindelse	V1.1	
Bilaga 2.1 Checklista för förbindelser med förhöjd säkerhet	V1.1	
Bilaga 3. Metod för anläggningsanalys	V1.1	

**Amendments:** Tillägg av Anvisningar för Anläggningar med förhöjd säkerhet utförda

**2024-03-01**

Datum 2024-03-01		
Dokument	Tidigare text	Tillägg eller reviderad text
<b>Huvuddokument</b>  <b>Bilaga 1 Robust site för samhällsviktig digital infrastruktur</b>  <b>Bilaga 2. Passiv säker fysisk förbindelse</b>  <b>Bilaga 3. Metod för anläggningsanalys</b>		Samtliga dokument har justerats och konsekvensuppdaterats avseende beteckningar av nivåerna för: <ul style="list-style-type: none"><li>• Säkerhetsnivåer</li><li>• Skyddsnivåer för förbindelser mellan siter</li><li>• Skyddsnivåer för anslutning</li></ul>
<b>Huvuddokument</b>		
3 Definitioner		<b>Komplettering</b> <b>Tillgångar</b> funktion som utgörs av en avgränsad del av ett kommunikationsnät eller en kommunikationstjänst och som är nödvändig för att tillhandahålla ett sådant nät eller en sådan tjänst, samt som används för att sända, motta, bearbeta eller lagra information, <b>Informationsbehandlingstillgångar</b> system, databaser och fysiska resurser som används för informationsbehandling, <b>Förbindelser</b> del av kommunikationsnät mellan två tillgångar eller mellan en tillgång och en anslutning till ett kommunikationsnät,
4.2 Fysisk och funktionell säkerhet		Tillägg <ul style="list-style-type: none"><li>• Den fysiska säkerheten omfattar åtgärder för att hantera fysiska hot mot tillgångar, informationsbehandlingstillgångar, förbindelser och system för styrning och övervakning. Fysiska hot kan till exempel omfatta stöld, brand, kabelbrott och strömavbrott. Även hot om brist på utrustning och reservdelar till kritiska nätverk och informationssystem omfattas*.</li><li>• Den funktionella säkerheten omfattar åtgärder för att hantera logiska hot mot tillgångar, informationsbehandlingstillgångar, förbindelser och system för styrning och övervakning.</li></ul>

<b>8.3.3 Skyddsnivåer för förbindelser mellan siter</b>	<b>Skyddsnivå SF1</b> Fysiska förbindelser med lägsta acceptabla säkerhet mellan noder i siter med skyddsnivå S0 och S1 eller S2.	<b>Skyddsnivå SF1</b> Fysiska förbindelser med <b>krav på bassäkerhet och redundans</b> lägsta acceptabla säkerhet mellan noder i siter med skyddsnivå S0 och S1 eller S2.
<b>10. RISK- OCH SÅRBARHETSANALYS (RSA)</b>		<b>Rubriken ädrad till 10 Hotkatalog, risk- och sårbarhetsanalys (RSA) och texten justerad så att den hanterar det nya Verkytet Hotkatalog, risk och sårbarhetsanalys för</b>
<b>Bilaga 1 Robust site för samhällsviktig digital infrastruktur</b>		
3 Hotbild		Rubriken ädrad till 3 <b>Hotkatalog, risk- och sårbarhetsanalys (RSA)</b> och texten justerad så att den hanterar det nya Verkytet Hotkatalog, risk och sårbarhetsanalys för
5.1.1 Områdesskydd	<b>Övergripande krav</b> Systemen för elektroniskt områdesskydd ska alltid vara anslutna till egen avbrottsfri kraft. anläggningens avbrottsfria kraft.	<b>Övergripande krav</b> <ul style="list-style-type: none"> <li>Systemen för elektroniskt områdesskydd ska alltid vara anslutna till <b>egen avbrottsfri kraft. anläggningens avbrottsfria kraft.</b></li> </ul>
5.1.1 Områdesskydd	<b>Tillträdeskontroll</b> Passerkontrollsystemet ska alltid ingå i en egen behörighetszon där den grupp av personer som har uttalade behov av tillträde till utrymmet ingår i en separat behörighetsgrupp.	<b>Tillträdeskontroll</b> <ul style="list-style-type: none"> <li>Passerkontrollsystemet ska alltid <b>omfatta ingå</b> i en egen behörighetszon där den grupp av personer som har uttalade behov av tillträde till utrymmet ingår i en separat behörighetsgrupp.</li> </ul>
5.2.1 Skalskydd		<b>Yttre placerad utrustning</b> Yttre placerad utrustning som t.ex anslutningsskåp inkommande serviceledning eller utanpåliggande delar av klimatanläggningen etc ska ha mekaniskt skydd mot yttre påverkan. Klassningen av skyddet ska motsvara <b>sitens klassning.</b>
5.2.5 Miljö och klimatskydd	<ul style="list-style-type: none"> <li>Nodutrymmet tillsammans med driftutrymmet ska generellt vara försett med ventilations- och kylanordning av typen "rumskyla" då utrymmet underskrider ca 50 kvm. Vid större utrymmen ska separat utredning utvisa lämpligt kylalternativ. Tilluft bör vara filtrerad med filter.</li> </ul>	<ul style="list-style-type: none"> <li>Nodutrymmet tillsammans med driftutrymmet ska generellt vara försett med ventilations- och kylanordning av typen "rumskyla" då utrymmet underskrider ca 50 kvm. Vid större utrymmen ska separat utredning utvisa lämpligt kylalternativ. Tilluft <b>ska bör</b> vara filtrerad med filter.</li> </ul>
5.2.5 Miljö och klimatskydd	<ul style="list-style-type: none"> <li>Klimatanläggningen ska övervakas lokalt i site och i Driftcentral och/eller</li> </ul>	<ul style="list-style-type: none"> <li>Klimatanläggningen ska övervakas lokalt i site och i Driftcentral och/eller Larmcentral (se kapitel 5.3 Driftlarm);</li> </ul>



	Larmcentral (se kapitel 5.3 Driftlarm): <ul style="list-style-type: none"> <li>Igensatta filter.</li> </ul>	<ul style="list-style-type: none"> <li>Igensatta filter.</li> </ul>
<b>5.2.8 Elinstallation</b>	<ul style="list-style-type: none"> <li>Varje UPS (om dubblerad) ska ha sina egna batterier. sitt eget batteri.</li> </ul>	<ul style="list-style-type: none"> <li>Varje UPS (om dubblerad) ska ha sina egna batterier. sitt eget batteri.</li> </ul>
<b>5.2.8 Elinstallation</b>	<ul style="list-style-type: none"> <li>Batterierna ska vara dimensionerade för att säkerställa el under den tid som åtgår för kontrollerad avstängning av utrustningen alternativt manuell start av reservkraft, dock minst 10 minuter. Beakta framtida utbyggnad vid dimensionering.</li> </ul>	<ul style="list-style-type: none"> <li>Batterierna ska vara dimensionerade för att säkerställa el under den tid som åtgår för kontrollerad avstängning av utrustningen alternativt manuell start av reservkraft, dock minst 10 minuter. Beakta framtida utbyggnad vid dimensionering.</li> </ul>
<b>5.2.8 Elinstallation</b>	Reservkraftsystem <ul style="list-style-type: none"> <li>Loggbok för bränsledieseltank ska finnas.</li> </ul>	Reservkraftsystem <ul style="list-style-type: none"> <li>Loggbok för bränsledieseltank ska finnas.</li> </ul>
<b>5.3 Driftlarm</b>	Funktionsövervakning och driftlarm ska hanteras över TCP/IP- förbindelser till Driftcentral och/eller Larmcentral.	Funktionsövervakning och driftlarm ska hanteras över TCP/IP- förbindelser till Driftcentral och/eller Larmcentral. Driftlarm ska även presenteras lokalt på anläggningen.
<b>9.1 Ett hållbart telekomsamhälle</b>		Kapitlet reviderat
<b>Bilaga 2. Passiv säker fysisk förbindelse</b>		
4 Hotbild		Rubriken ädrad till 4 Hotkatalog, risk- och sårbarhetsanalys (RSA) och texten justerad så att den hanterar det nya Verktuget Hotkatalog, risk och sårbarhetsanalys för
5.2.2 (6.3.1) Förbindelser mellan anläggningar	<b>5.2.2 Förbindelser mellan anläggningar</b> Skyddsnivå SF1. Fysiska förbindelser med minimikrav för säkerhet mellan noder i siter med skyddsnivå S0 och S1 eller S2.	Skyddsnivå SF1. Fysiska förbindelser med krav på bassäkerhet och redundans minimikrav för säkerhet mellan noder i siter med skyddsnivå S0 och S1 eller S2.
6.4.4.1 Kabelbrunn (typ 0)		Ny pos Tillägg av brunstyp 0
6.4.5.1 Bassäkerhet skyddsåtgärder markskåp (typ 1)	Markskåp bör förses med ett system för fjärrövervakning avseende kontroll och larm för: <ul style="list-style-type: none"> <li>Öppen/stängd lucka/dörr</li> <li>Yttre åverkan/vandalisering</li> </ul>	Markskåp bör förses med ett system för fjärrövervakning avseende kontroll och larm för: <ul style="list-style-type: none"> <li>Öppen/stängd lucka/dörr</li> <li>Yttre åverkan/vandalisering</li> </ul>



6.4.5.1 Bassäkerhet skyddsåtgärder markskåp (typ 1)	Det ska inte gå att utifrån skruva isär ett markskåp: Om markskåpet är försett med gångjärn ska dessa var dolda.	Krav borttagna från bassäkerhet Det ska inte gå att utifrån skruva isär ett markskåp. Om markskåpet är försett med gångjärn ska dessa var dolda.
6.4.5.3 Hög säkerhet, skyddsåtgärder markskåp		Om markskåpet är försett med gångjärn ska dessa var dolda.
7. SÄKERHETSMATRIS		Justering efter korrigeringar
<b>Bilaga 3. Metod för anläggningsanalys</b>		Konsekvensuppdateringar avseende justerade säkerhets-och skyddsnivåer.

