

Vitbok för Riktlinjer för säkerhet i telenät och teletjänster

Ver. 1.2

TLP:CLEAR



Innehåll

Syfte med vitboken.....	2
1 Kompletterande begreppsförklaringar.....	3
2 Mappning.....	4
3 Utdrag ur CSL.....	5
3.1 Utbildning Säkerhetsåtgärder.....	5
4 Branschförkortningar.....	6
4.1 Begrepp.....	6
4.2 System.....	8
4.3 Organisationer och funktioner.....	8



Syfte med vitboken

Vitbokens syfte är att vara en komplettering till Riktlinjerna med utökad information om lagar, författningar och anvisningar och de begrep och definitioner som ingår i dessa.

Den innehåller också en mappning från **Ledningssystem för driftsäkerhet** till **Riktlinjer för Telenät och Teletjänster**.

Vitboken kommer succesivt kompletteras med användarnas uppkomna frågeställningar och vägledning till svar.



1 Kompletterande begreppsförklaringar

Förklaringar på begrepp som förekommer i lagtexter, föreskrifter och andra dokument som Riktlinjerna hänvisar till, men som inte behandlas i Riktlinjerna.

datacentraltjänst: en tjänst som omfattar strukturer, eller grupper av strukturer, avsedda för centraliserad inkvartering, sammankoppling och drift av sådan it- och nätutrustning som tillhandahåller datalagrings-, databehandlings- och dataöverföringstjänster samt alla anläggningar och infrastrukturer för kraftdistribution och miljökontroll,

domännamnsregistreringstjänster: registrerar eller en annan verksamhetsutövare som verkar som ombud eller återförsäljare av domännamn,

Domännamssystemtjänst: en allmän rekursiv tjänst för att lösa domännamnsfrågor till internetslutanvändare, eller en auktoritativ tjänst för att lösa domännamnsfrågor för användning av tredje part, med undantag för rotnamnservrar,

domännamssystem (DNS): ett hierarkiskt distribuerat namnsystem som möjliggör identifieringen av tjänster och resurser på internet,

domännamssystemtjänster (DNS-tjänster): allmänna rekursiva tjänster för att lösa domännamnsfrågor till internetslutanvändare, eller auktoritativa tjänster för att lösa domännamnsfrågor för användning av tredje part, med undantag för rotnamnservrar,

IKT-produkt, IKT-tjänst och IKT-process: enligt begreppens definitioner i artiklarna 2.12, 2.13 och 2.14 i Cybersäkerhetsakten,

Kvalificerade tillhandahållare av betrodda tjänster: begreppet har samma innebörd som i Europaparlamentets och rådets förordning (EU) nr 910/2014 av den 23 juli 2014 om elektronisk identifiering och betrodda tjänster för elektroniska transaktioner på den inre marknaden och om upphävande av direktiv 1999/93/EG,

Nätverk för leverans av innehåll: ett nätverk av geografiskt spridda servrar vars syfte är att säkerställa hög tillgänglighet för, tillgång till eller snabb leverans av digitalt innehåll och digitala tjänster till internetanvändare för innehålls- och tjänsteleverantörers räkning,

Plattform för sociala nätverkstjänster: en plattform som gör det möjligt för slutanvändare att interagera, dela och upptäcka innehåll, finna andra användare och kommunicera med andra via flera enheter, exempelvis genom chattar, inlägg, videor och rekommendationer,

Registreringsenhet för toppdomäner: en verksamhetsutövare som har delegerats en specifik toppdomän och som ansvarar för administrationen av den, dock inte om toppdomänen används endast för registreringsenhetens eget bruk,

Sökmotor: detsamma som i artikel 2.5 i Europaparlamentets och rådets förordning (EU) 2019/1150 av den 20 juni 2019 om främjande av rättvisa villkor och transparens för företagsanvändare av onlinebaserade förmedlingstjänster,

Tillbud: en händelse som kunde ha undergrävt tillgängligheten, autenticiteten, riktigheten eller konfidentialiteten hos lagrade, överförda eller behandlade uppgifter eller hos de tjänster som erbjuds genom eller är tillgängliga via nätverks- och informationssystem, men som framgångsrikt hindrades från att utvecklas eller som inte uppstod, SOU 2024:18 Författningsförslag.



2 Mappning

Detta är en mappning från **Ledningssystem för driftsäkerhet** till de nya **Riktlinjerna för säkerhet i telenät och teletjänster**.

Ämnesområde	Ledningssystem för driftsäkerhet	Riktlinjerna för säkerhet i telenät och teletjänster
Definitioner	-	Bilaga
Syfte	Kap 3	Kap 2
Verksamhetsbeskrivning	-	Kap 3
Verksamhetsplan	-	Kap 4
Organisation	Kap 4	Kap 5
Medarbetare/Utbildning	Kap 5	Kap 17
Dokumentation - tillgångar och förbindelser	Kap 6.1.1	Kap 7
Uppdragstagare /Leverantörshantering	Kap 6.1.2	Kap 14.3
Dokumentation - bevarande av dokumentation	Kap 6.1.3	Kap 7
Risکانالys för tillgångar och förbindelser	Kap 6.2	Kap 13
Risکانالys förändring	Kap 6.2.1	Kap 11
Upphandling/Anskaffningskontroll	Kap 6.2.2	Kap 10.2
Riskbedömning och förändringshantering	Kap 6.3	Kap 13
Åtkomst och behörighet	Kap 6.4	Kap 14.1
Övervakning	Kap 6.5	Kap 14.1.4
Beredskap	Kap 6.5	Kap 8.1
Konsekvensanalys	Kap 7.1	Kap 13.3
Incidenthantering	Kap 7.2	Kap 12.1
Kontinuitetsplan/kontinuitetshantering	Kap 7.2	Kap 15.1
Kontroll, Uppföljning, Utvärdering och förbättringar	Kap 8	Kap 18
Övningsverksamhet	Kap 9	Kap 15.1
Förvaltning av dokumenten för Ledningssystem för driftsäkerhet/Riktlinjerna	Kap 10	Kap 5.3
Nätarkitektur, Teletjänster och kapacitet	-	Kap 6
Driftenhet Nät och tjänster	-	Kap 8.1
Driftenhet IT	-	Kap 8.2
Förebyggande underhåll	-	Kap 9.1
Reservdelshantering	-	Kap 9.2
Uppdatering av mjukvara	-	Kap 9.3
Akut underhåll	-	Kap 9.4
Anskaffningsrutiner	-	Kap 10.1
Integritetsincident	-	Kap 12.1.2
Rapportering Integritetsincident	-	Kap 12.2
Säkerhetshantering	-	Kap 14
Skyddsåtgärder för information		Kap 14.2
Fysisk säkerhet	-	Kap 14.1
Extern kommunikation	-	Kap 16



3 Utdrag ur CSL

I detta kapitel finns hänvisningen till Cybersäkerhetslagen.

3.1 Utbildning Säkerhetsåtgärder

Cybersäkerhetslagen (2025:1506)

2 kap. Verksamhetsutövares skyldigheter

Utbildning

4 § De personer som ingår i ledningen för en verksamhetsutövare ska genomgå utbildning om säkerhetsåtgärder.

Kommentar:

Cybersäkerhetslagen bygger på NIS2-direktivets krav att ledningsorgan ska:

- godkänna organisationens cybersäkerhetsåtgärder,
- övervaka genomförandet,
- ha tillräcklig kunskap för att kunna utöva sitt ansvar.

I praktiken innebär detta att styrelse, VD, förvaltningsledning, nämndledning eller motsvarande måste genomgå utbildning som ger förståelse för:

- cyberrisker,
- säkerhetsåtgärder,
- incidenthantering,
- rapporteringsskyldigheter,
- verksamhetens ansvar enligt lagen.

Det räcker alltså inte att ledningen "har tillgång till experter". Ledningen måste själv ha dokumenterad kompetens för att kunna fatta informerade beslut.



4 Branschförkortningar

Detta är en lista på förekommande förkortningar i lagar, förordningar, artiklar, utbildningar, litteratur, hemsidor, standarder etc.

I listan finns både engelska och svenska förkortningar och ibland både den svenska och engelska för samma begrepp.

4.1 Begrepp

BCM	Business Continuity Management (Kontinuitetshantering)
BCMS	Business Continuity Management Systems
BCP	Business Continuity Plan (Kontinuitetsplan)
CDN	Content Delivery Network (nätverk för leverans av innehåll)
CER-direktivet	Critical Entities Resilience (resiliens hos kritiska enheter)
COBIT	Control Objectives for Information and Related Technologies
CPS	Cyber-Physical Systems (cyberfysiska system)
CRA	Cyber Resilience Act (EU-direktiv)
CRM	Customer Relationship Management
CSL	Cybersäkerhetslagen
Cybersäkerhet	Att skydda nätverk, datorer och information från att bli skadade, hackade eller stulna.
DDoS	Distributed Denial of Service. DDoS-attacker är övebelastningsatacker.
DMA	Digital Services Act (EU-direktiv)
DNA	Digital Networks Act (EU-direktiv)
DNS	Domain Name System
DRP	Disaster Recovery Plan
Dora	Digital Operational Resilience Act
DSA	Digital Services Act (EU-direktiv)
eIDAS	electronic IDentification, Authentication and trust Services
FRA	Försvarets Radioanstalt
FS	Författningssamling
GDPR	General Data Protection Regulation (Allmän dataskyddsförordning)
GIA	Gigabit Infrastructure Act (EU-direktiv)
IaaS	Infrastructure as a Service
ICS	Industrial Control System (industriella informations- och styrsystem)
ICT	Information and Communication Technology (IKT på svenska)
IdP	Identity Provider



IKT	Informations- och kommunikationsteknik (ICT på engelska)
IOC	Indicators of Compromise (Angreppsindikation)
IoT	Internet of Things
IPS	Intrusion prevention systems
ISP	Internet Service Provider
IT	Information Technology
ITIL	Information Technology Infrastructure Library
IXP	Internetknutpunkt
KPI	Key Performance Indicator
LEK	Lagen om Elektronisk Kommunikation
LER	Label Edge Router
LSP	Label Switched Path
LSR	Label Switching Router
M2M	Machine to Machine
MFA	Multifaktorautentisering
MITM	Man in the middle
MPLS	Multiprotocol Label Switching
MTBF	Mean Time Between Failures
MTTR	Mean Time To Repair
MWT	Mean Waiting Time
NIS	Network and Information Security
NOC	Network Operations Center
OT	Operational Technology (hårdvara/mjukvara för övervakning och styrning av industriella system och processer)
PaaS	Platform as a Service
PLC	Programmable Logic Controller
QoS	Quality of Service
RAN	Radio Access Network - Radioaccessnät
RDI	Robust Digital Infrastruktur
RPO	Recovery Point Objective
RTO	Recovery Time Objective
RTU	Remote Terminal Unit
SaaS	Software as a Service
SDK	Säker digital kommunikation (Digg)
SIEM	Security Information and Event Management



SCADA	Supervisory Control and Data Acquisition (en central roll i OT)
SOC	Security Operations Center
SOU	Statens offentliga Utredning
SSA	Systematisk säkerhetsarbete
SSO	Single Sign-On
TLD	Top Level Domain (Toppdomän till exempel .com .org .se .nu .eu)
UPS	Uninterruptible Power Supply
WIS	Webbaserat informationssystem
XDR	Extended Detection and Response

4.2 System

BSS	Business Support Systems
CRISIS	Critical Response and Incident System Information Sharing
IDS	Intrusion detection systems
IPS	Intrusion prevention systems
HVAK	Heating, Ventilation and Air Conditioning
MISP	Malware Information Sharing Platform & Threat Sharing (används av CERT och SCIRT)
NMS	Network Security Monitor - Nätverksövervakningssystem
OSS	Operations Support Systems
RTU	Remote Terminal Unit (bearbetar sensorinformation innan kommunikation)

4.3 Organisationer och funktioner

CERT	Computer Emergency Response Team
CERT-SE	Computer Emergency Response Team Sweden (MCF:s CSIRT)
CISO	Chief Information Security Officer
CSA	Cloud Security Alliance
CSIRT	Computer Security Incident Response Team (hanterar och förebygger IT-incidenter)
ENISA	The European Union Agency for Cybersecurity
EEG	Europeiska ekonomiska gemenskapen
EES	Europeiska ekonomiska samarbetsområdet
EFTA	Europeiska frihandelssammanslutningen
EG	Europeiska gemenskaperna (föregångaren till EU)
ENISA	Europeiska unionens cybersäkerhetsbyrå
ETSI	European Telecommunications Standards Institute



EU	Europeiska unionen
EU-CyCLONe	EU Cyber Crises Liaison Organisation Network (hantera och samordna responsen på större cyberkriser)
FOI	Totalförsvarets forskningsinstitut
FRA	Försvarets Radioanstalt
IANA	Internet Assigned Numbers Authority
ICANN	Internet Corporation for Assigned Names and Numbers
IMY	Integritetsskyddsmyndigheten
MCF	Myndigheten för civilt försvar (fd. MSB)
MHS	Militärhögskolan
NCSC	Nationellt Cybersäkerhetscenter (del av FRA)
NIST	National Institute of Standards and Technology
NTSG	Nationella Telesamverkansgruppen
PTS	Post- och Telestyrelsen (<i>byter namn 2027-01-01 till Digitaliseringsmyndigheten</i>)
SISG	Stadsnätens infrastruktursamverkansgrupp
SKR	Sveriges kommuner och regioner
SOC	Security Operations Center
SÄPO	Säkerhetspolisen
UND	Sveriges utrikes underrättelsetjänst

