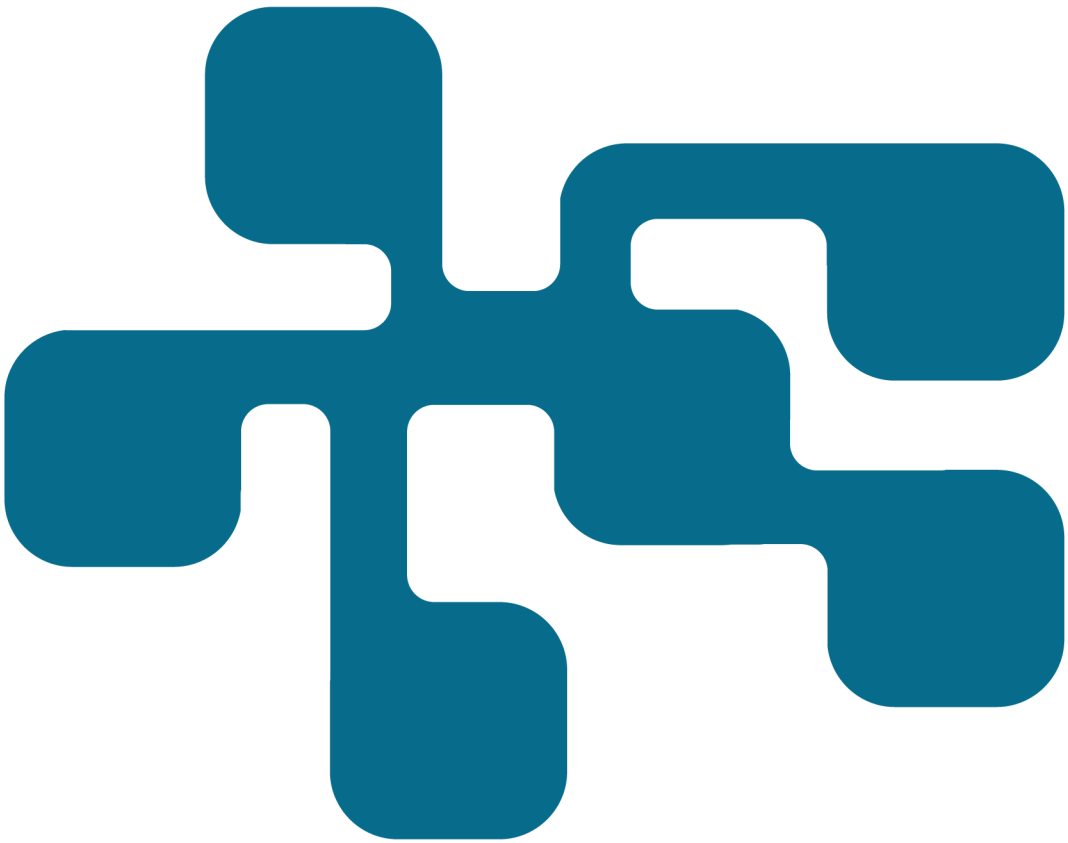
NCS3 - Regelverk och krav inom området industriella informations- och styrsystem

En uppdatering av utvecklingen sedan december 2015

Jessica Appelgren, Erik Zouave

FOI
MSB



FOI-R--5073--SE
MSB 2020-04491
ISSN 1650-1942

Mars 2021

Jessica Appelgren, Erik Zouave

NCS3 - Regelverk och krav inom området industriella informations- och styrsystem

En uppdatering av utvecklingen sedan december 2015

Titel	NCS3 - Regelverk och krav inom området industriella informations- och styrsystem – En uppdatering av utvecklingen sedan december 2015
Title	NCS3 – Swedish Regulations within the area of Industrial Control Systems
Rapportnr	FOI-R--5073--SE
Månad	Mars
Utgivningsår	2021
Antal sidor	67
ISSN	1650-1942
Kund	Myndigheten för samhällsskydd och beredskap
Forskningsområde	Krisberedskap och civilt försvar
FoT-område	Inget FoT-område
Projektnr	E13729
Godkänd av	Malek Finn Kahn
Ansvarig avdelning	Försvarsanalys

Sammanfattning

Totalförsvarets forskningsinstitut (FOI) genomförde under 2012, på uppdrag av Myndigheten för samhällsskydd och beredskap (MSB), en studie i syfte att undersöka hur regelverk och krav styr säkerhetsarbetet med industriella informations- och styrsystem. Studien omfattade sektorerna: elproduktion och eldistribution, dricksvatten, fjärrvärme och fjärrkyla, kemisk processindustri, spårbunden trafik, samt elektroniska kommunikationer. 2015 genomförde FOI en uppdatering av studien för att följa upp vilka förändringar inom regelverk och krav som skett för respektive sektor sedan december 2012.

Regelverk och krav som styr säkerhetsarbetet med industriella informations- och styrsystem har sedan förändrats genom omfattande reformer. Detta gäller i synnerhet med antagandet av NIS-direktivet, cybersäkerhetsakten och nya säkerhetsskyddslagen. I denna rapport redovisas resultatet från en uppföljande studie med målet att på övergripande nivå beskriva nu gällande regelverk och krav för industriella informations- och styrsystem, genom att inkludera de förändringar som genomförts efter den 1 december 2015. Förutom tidigare kartlagda sektorer har denna rapport utökats med sektorn hälso- och sjukvård.

Rapporten beskriver både relevanta regelverk och krav för respektive utpekad sektor och centrala sektorsövergripande regelverk och krav. Rapporten ger även exempel på ett antal lagar och bestämmelser inom andra områden som kan påverka både krav som generellt ställs på informationssäkerhet, såväl som på informations- och styrsystem.

Nyckelord: Regelverk, krav, informations- och styrsystem, kontrollsystem, cybersäkerhetsakten, dataskydd, informationssäkerhet, säkerhetsskydd, informations- och kommunikationsteknik, SCADA-system, elproduktion, eldistribution, dricksvattenproduktion, vattendistribution, fjärrvärme, fjärrkyla, kemisk processindustri, spårbunden trafik, elektroniska kommunikationer, hälso- och sjukvård.

Summary

In 2012, the Swedish Defence Research Agency (FOI) carried out a study, on behalf of the Swedish Civil Contingencies Agency (MSB), to investigate how regulations and requirements govern security work within industrial information and control systems. The study covered the sectors: electricity production and electricity distribution, drinking water, district heating and cooling, chemical process industry, rail traffic and electronic communications. In 2015, FOI conducted a study to follow up on changes since 2012.

Regulations and requirements that govern security work within industrial information and control systems have since changed through extensive reforms. This applies in particular to the adoption of the NIS Directive, the EU Cybersecurity Act and the Protective Security Act. This report presents a follow-up study with the aim of describing, at an overall level, current regulations and requirements, by including changes implemented after 1 December 2015. In addition to previously mapped sectors, this report includes the healthcare sector.

The report describes both relevant regulations and requirements for each designated sector and central sector-wide regulations and requirements. It also provides examples of laws and regulations in other areas that may affect both requirements that are generally placed on information security, as well as on information and control systems.

Keywords: Regulations, requirements, information and control systems, control systems, cybersecurity act, data protection, information security, security protection, information and communication technology, SCADA systems, electricity production, electricity distribution, drinking water production, water distribution, district heating, district cooling, chemical process industry, rail communications, electronic communications, healthcare.

Innehåll

1 Inledning

1.1 Bakgrund

Totalförsvarets forskningsinstitut (FOI) genomförde under 2012, på uppdrag av Myndigheten för samhällsskydd och beredskap (MSB), en studie [1] i syfte att undersöka hur regelverk och krav styr säkerhetsarbetet med industriella informations- och styrsystem. Studien omfattade sektorerna: elproduktion och eldistribution, dricksvatten, fjärrvärme och fjärrkyla, kemisk processindustri, spårbunden trafik samt elektroniska kommunikationer. 2015 initierade MSB en uppdatering[2] av studien för att följa upp vad som hänt inom sektorerna sedan december 2012.

De regelverk och krav som styr säkerhetsarbetet med industriella informations- och styrsystem har sedan dess förändrats genom omfattande reformer. Detta i synnerhet med antagandet av NIS-direktivet[3] som fastställer åtgärder för säkerhet i nätverks- och informationssystem i samhällsviktig verksamhet. På sektorsövergripande nivå har även exempelvis cybersäkerhetsakten[4] med harmonisering av europeisk standardisering, certifiering och ackreditering av informations- och kommunikationsteknik (IKT) samt den nya säkerhetsskyddslagen[5], med krav på informationssäkerhet och fysisk säkerhet för styrsystem tillkommit.

Under 2020 beslutade MSB därför att göra en uppföljande studie med syfte att inkludera förändringar i regelverk och krav som har genomförts efter den 1 december 2015 med bäring på säkerhet i industriella informations- och styrsystem. Studien, vars resultat redovisas i den här rapporten, omfattar de tidigare kartlagda sektorerna samt har utökats med sektorn hälso- och sjukvård.

[1] Lindgren, F. (2013). Regelverk och krav inom området säkerhet i industriella informations- och styrsystem. FOI Memo 4415.

[2] Mossberg Sonnek, K och Lindgren, F. (2015). NCS3 – Regelverk och krav inom området industriella informations- och styrsystem. FOI-R--4197--SE.

[3] Europaparlamentets och Rådets Direktiv (EU) 2016/1148 av den 6 juli 2016 om åtgärder för en hög gemensam nivå på säkerhet i nätverks- och informationssystem i hela unionen. Den 16 december 2020 presenterade EU-kommissionen ett förslag på ett nytt NIS-direktiv, kallat NIS 2, med syftet att anpassa direktivet till nya och framtida behov. Förslaget har ännu inte (210201) fastställts, utan har lämnats för beredning till rådet och EU-parlamentet. Läs mer om direktivet på https://ec.europa.eu/digital-single-market/en/news/proposal-directive-measures-high-common-level-cybersecurity-across-union.

[4] Förslag till Europaparlamentets och Rådets Förordning om Enisa, ”EU:s cybersäkerhetsbyrå”, och om upphävande av förordning (EU) nr 526/2013, och om cybersäkerhetscertifiering av informations- och kommunikationsteknik (”cybersäkerhetsakten”). COM/2017/0477 final/2 - 2017/0225 (COD).

[5] Säkerhetsskyddslag (2018:585)

1.2 Syfte

Lagstiftningen är en central del av det svenska och europeiska informations- och cybersäkerhetsarbetet och berör samtliga aktörer som arbetar med dessa frågor. Lagstiftningen förser dessutom aktörer inom samhällsviktig verksamhet med det underlag de behöver för att bedriva sitt säkerhetsarbete på ett sätt som inte skapar oönskade effekter för individens integritet, dess fri- och rättigheter vid behandlingen av personuppgifter och främjar förtroende, trygghet och tillit till det digitaliserade samhället. Syftet med studien är även att den ska fungera som en referensbank för MSB:s program[6] för ökad säkerhet i industriella informations- och styrsystem.

Målet med denna rapport är att på en övergripande nivå beskriva nu gällande regelverk och krav för industriella informations- och styrsystem inom sektorerna:

- Elproduktion och eldistribution.
- Dricksvattenproduktion och vattendistribution.
- Fjärrvärme/-kyla – produktion och distribution.
- Kemisk processindustri.
- Spårbunden trafik.
- Elektroniska kommunikationer.
- Hälso- och sjukvård.

1.3 Målgrupp

Målgrupp för rapporten är de som arbetar med frågor relaterade till informationssäkerhet, it-säkerhet eller styrsystem och är verksamma inom de sektorer som studien berör samt övriga med intresse för regelverk och krav relaterade till industriella informations- och styrsystem.

1.4 Metod och avgränsningar

Denna rapport uppdaterar den föregående rapporten *NCS3 – Regelverk och krav inom området industriella informations- och styrsystem (FOI-R--4197--SE).* [7] Uppdateringen tar särskilt höjd för att cybersäkerhetsakten, NIS-direktivet samt säkerhetsskyddslagen har tillkommit sedan föregående rapport. Genom att utgå från de förändringar som genomförts sedan december 2015 ska rapporten på en övergripande nivå redogöra för gällande regelverk (lagar, direktiv, förordningar,

[6] Läs mer på https://www.msb.se/sv/amnesomraden/informationssakerhet-cybersakerhet-och-sakra-kommunikationer/sakerhet-i-cyberfysiska-system/industriella-information--och-styrsystem/ (Besökt 21-01-13)

[7] Mossberg Sonnek, K och Lindgren, F. (2015). NCS3 – Regelverk och krav inom området industriella informations- och styrsystem. FOI-R--4197--SE.

föreskrifter med mera) och säkerhetskrav för verksamhet med industriella styrsystem i samhällsviktiga sektorer.

I rapporten har främst svenska lagar, förordningar och föreskrifter studerats.[8] Därtill har eventuella vägledningar och handböcker med koppling till nämnda författningar granskats. Vidare har Europeiska unionens (EU:s) rättsakter, förordningar och direktiv av relevans för området studerats. I studien granskades även underlaget i den tidigare rapporten (FOI-R--4197--SE) för att bedöma omfattning av vilka regelverk och krav som skulle inkluderas i studien.

Genomgången har inte som ambition att vara komplett, men kan ses som en generell överblick av vilka regelverk och krav som finns inom de studerade sektorerna idag. Rapporten innehåller inte heller, på grund av utrymmesskäl och tidsåtgång, någon fullständig redovisning av innehållet i de regelverk och övrigt material som nämns, men åtskilliga exempel ges på detaljbestämmelser.

1.5 Rapportens disposition

Rapporten inleds med centrala sektorsövergripande regelverk och krav. Därefter beskrivs relevanta regelverk och krav enskilt för var och en av de utpekade sektorerna. Rapporten avslutas med exempel på ett antal lagar och bestämmelser inom andra områden som kan påverka både de krav som generellt ställs på informationssäkerhet, såväl som på informations- och styrsystem. I slutet av rapporten finns en ordlista med förklaringar av vissa av de juridiska termer som nämns i rapporten. Referenser finns såväl i fotnoter som i den löpande texten och är även samlade kapitelvis längst bak i rapporten.

[8] Den främsta källan för dessa är https://www.riksdagen.se/sv/dokument-lagar/

2 Sektorsövergripande reglering

Sedan publiceringen av *NCS3 – Regelverk och krav inom området industriella informations- och styrsystem (FOI-R--4197--SE)*[9] har omfattande rättsliga reformer medfört utökade krav på säkerhet för informations- och styrsystem. Merparten av dessa krav har införts genom teknikneutral, sektorsövergripande reglering. Teknikneutraliteten innebär att regleringen inte specifikt riktar sig mot informations- och styrsystem, specifika tekniska komponenter av dessa, eller all verksamhet med dessa. Istället tar regleringen sikte på ett antal typer av verksamhet och teknik där informations- och styrsystem kan ingå.

2.1 Cybersäkerhetsakten

Under 2019 antogs Europeiska kommissionens förordning (EU) 2019/881, även kallad ”cybersäkerhetsakten”.[10] Cybersäkerhetsakten syftar till att åstadkomma en hög nivå av cybersäkerhet och cyberresiliens i europeisk informations- och kommunikationsprodukter, -tjänster, och -processer (IKT i denna rapport).[11] Säkerhetskraven inom cybersäkerhetsakten uppnås främst genom det löpande upprättandet av europeiska och nationella ordningar för cybersäkerhetscertifiering[12].

Cybersäkerhetsakten skiljer sig från andra lagar i denna rapport då den inte upprättar egna cybersäkerhetskrav utan istället inrättar ett ramverk för frivillig cybersäkerhetscertifiering. Cybersäkerhet är ”all verksamhet som är nödvändig för att skydda nätverks- och informationssystem, användare av dessa system och andra berörda personer” mot möjliga handlingar, omständigheter, eller händelser som på ett negativt sätt påverkar nätverks- och informationssystemen och människor.[13]

---

[9] Mossberg Sonnek, K och Lindgren, F. (2015). NCS3 – Regelverk och krav inom området industriella informations- och styrsystem. FOI-R--4197--SE.

[10] Europaparlamentets och rådets förordning (EU) 2019/881 av den 17 april 2019 om Enisa (Europeiska unionens cybersäkerhetsbyrå) och om cybersäkerhetscertifiering av informations- och kommunikationsteknik och om upphävande av förordning (EU) nr 526/2013 (cybersäkerhetsakten) (Text av betydelse för EES) PE/86/2018/REV/1. EUT L 151.

[11] Artikel 1, förordning (EU) 2019/881; Förslag till Europaparlamentets och Rådets förordning om Enisa, ”EU:s cybersäkerhetsbyrå”, och om upphävande av förordning (EU) nr 526/2013, och om cybersäkerhetscertifiering av informations- och kommunikationsteknik (”cybersäkerhetsakten”). COM(2017) 477 final.

[12] Artikel 2 p.9-10, förordning (EU) 2019/881, Europeisk ordning för cybersäkerhetscertifiering beskrivs som ”en vittomfattande uppsättning regler, tekniska krav, standarder och förfaranden som fastställs på unionsnivå och som tillämpas på certifiering eller bedömning av överensstämmelse av särskilda IKT-produkter, IKT-tjänster och IKT-processer.” Nationell ordning för cybersäkerhetscertifiering beskrivs som ”en komplett uppsättning regler, tekniska krav, standarder och förfaranden som utvecklas och antas av en nationell offentlig myndighet och som tillämpas vid certifiering eller vid bedömning av överensstämmelse av IKT-produkter, IKT-tjänster och IKT-processer som omfattas av tillämpningsområdet för den ordningen.”

[13] Artikel 2, förordning (EU) 2019/881.

Cybersäkerhetscertifieringsordningarna däremot kommer att bestämma detaljerna kring cybersäkerhetskraven. De kommer bland annat förtydliga regler, tekniska krav, standarder och förfaranden, bedömningskriterier och metoder för cybersäkerhet i IKT, samt eventuella bestämmelser för rapportering av tidigare oupptäckta sårbarheter med mera.[14] Certifieringsordningarna kommer att utarbetas utifrån ett antal gemensamma målsättningar för IKT:

- Skydd av data mot oavsiktlig eller otillåten lagring, behandling, åtkomst, offentliggörande, ändringar, eller brist på tillgänglighet under hela livscykeln för IKT.
- Åtkomsträttigheter som säkerställer att endast behöriga personer, program eller maskiner kan få åtkomst till data, tjänster eller funktioner.
- Identifiering och dokumentering av sårbarheter och beroenden, samt kontroll av sårbarheter i IKT.
- Registrering av vilka data, tjänster och funktioner som någon haft åtkomst till eller behandlat, och när.
- Möjligheten att återställa tillgängligheten av data, tjänster och funktioner vid en incident.
- Säkert grundutförande och konstruktion för IKT.
- Säker uppdatering av programvara och maskinvara för IKT som innehåller kända sårbarheter.[15]

Europeiska unionens cybersäkerhetsbyrå (Enisa) kommer att anta dessa certifieringsordningar på begäran av Europeiska kommissionen. Kommissionen meddelar löpande en förteckning över vilka kategorier av IKT som kommer regleras av certifieringsordningarna. EU:s medlemsstater får även meddela egna certifieringsordningar där det inte redan finns en europeisk ordning.[16]

Regleringen omfattar delar av nätverks- och informationssystem, alla tjänster som i huvudsak innefattar överföring, lagring, hämtning eller behandling av information via dessa system, eller verksamheten för utformning, utveckling, eller tillhandahållande av systemen och tjänsterna.[17] Regleringen omfattar också sakernas internet och industriella informations- och styrsystem. I förslaget om en cybersäkerhetsakt bedömde Kommissionen att certifieringen skulle vara särskilt relevant för sakernas internet och industriella automatiseringskontrollsystem (IACS).[18] Även om den slutliga cybersäkerhetsakten inte återger en uttömmande

[14] Artiklarna 2 och 54, förordning (EU) 2019/881.
[15] Artikel 51, förordning (EU) 2019/881.
[16] Artiklarna 47-50 och 57, förordning (EU) 2019/881.
[17] Artikel 2, förordning (EU) 2019/881.
[18] Förslag till Europaparlamentets och Rådets förordning om Enisa, ”EU:s cybersäkerhetsbyrå”, och om upphävande av förordning (EU) nr 526/2013, och om cybersäkerhetscertifiering av informations- och kommunikationsteknik (”cybersäkerhetsakten”), s. 2, 9, 10, 33, skäl 48; COM(2017) 477 final; Meddelande från Kommissionen till Europaparlamentet, Rådet, Europeiska Ekonomiska och Sociala

lista för vilka styrsystem som kan komma att täckas av ordningar för cybersäkerhetscertifiering, ger skäl 65 av akten en (icke uttömmande) fingervisning om detta:

> Uppkopplade och automatiserade bilar, elektroniska medicintekniska produkter, styrsystem för industriell automation och smarta elnät är bara några exempel på sektorer inom vilka certifiering redan används eller kan komma att användas i en nära framtid.[19]

Dessutom ska cybersäkerhetscertifieringsordningarna även rikta sig mot system som används i samhällsviktiga tjänster.[20] Leverantörer av samhällsviktiga tjänster enligt NIS (bland annat inom sektorerna el, dricksvatten, spårbunden trafik) bör förvänta sig att särskilda, obligatoriska cybersäkerhetskrav på sikt kommer att utvecklas för deras verksamhet via certifieringsordningarna.[21] Kraven kommer således bli skarpare för denna verksamhet än för övrig, frivillig certifiering.

I skrivande stund är cybersäkerhetsaktens genomförande i Sverige inte fullt utvecklad. Exempelvis är det inte beslutat vilken myndighet som kommer vara nationell myndighet för cybersäkerhetscertifiering.[22]

2.2 Dataskyddet

Dataskyddet är ett skydd av fysiska personers (individers) rättigheter vid behandlingen av personuppgifter.[23] Dataskyddet är reglerat i artikel 8 till Europeiska unionens stadga om de grundläggande rättigheterna,[24] förordning (EU) 2016/679 (GDPR), lag med kompletterande bestämmelser till EU:s dataskyddsförordning,[25] samt utlåtanden från Europeiska dataskyddsstyrelsen, Datainspektionen, samt utlåtanden från övriga dataskyddsmyndigheter i EU:s medlemsstater. Lagarna reglerar, bland annat, säkerhetskrav vid alla typer av manuella eller automatiserade åtgärder (behandling) av personuppgifter, det vill säga uppgifter som avser identifierade eller identifierbara individer (registrerade).

Dataskyddet har haft bred inverkan på säkerheten i informationssystem eftersom dessa system ofta innefattar funktioner med personuppgiftsbehandling. Data-

---

Kommittén samt regionkommittén. Prioriteringar för informations- och kommunikationsteknisk standardisering på den digitala inre marknaden. COM/2016/0176 final.

[19] Skäl 65, förordning (EU) 2019/881.

[20] Skäl 65, förordning (EU) 2019/881.

[21] Skäl 92, förordning (EU) 2019/881.

[22] Kommittédirektiv Cybersäkerhet – genomförandet av cybersäkerhetsakten och vissa åtgärder till skydd för säkerhetskänslig verksamhet. Dir. 2019:73.

[23] Artikel 1, Europaparlamentets och rådets förordning (EU) 2016/679 av den 27 april 2016 om skydd för fysiska personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter och om upphävande av direktiv 95/46/EG (allmän dataskyddsförordning) (Text av betydelse för EES) EUT L 119, 4.5.2016.

[24] Europeiska unionens stadga om de grundläggande rättigheterna. EUT C 326.

[25] Lag (2018:218) med kompletterande bestämmelser till EU:s dataskyddsförordning.

skyddets relevans för styrsystem är något mer begränsad då dessa system inte behandlar personuppgifter i samma omfattning. Det finns dock anledning att sammanställa dataskyddets krav i denna rapport:

- Det finns industriella styrsystem som behandlar personuppgifter.[26]
- Dataskyddet gäller även för behandling på arbetsplatsen och anställdas integritet,[27] exempelvis behörighetskontroller för informationssäkerhet.
- Dataskyddet gäller även vid informationssäkerhet för samhällsviktig verksamhet.[28]

Säkerheten vid behandlingen av personuppgifter baseras på principen om integritet och konfidentialitet avseende skyldigheter för säkerhet vid personuppgiftsbehandling. Sammantaget innebär dessa regler att personuppgifter ska behandlas med lämpliga tekniska och organisatoriska åtgärder för att skydda mot obehörig åtkomst, röjning, delning, ändring, förlust och förstöring av personuppgifter (personuppgiftsincidenter).[29] Datainspektionen har även fastställt allmänna råd om säkerhet för personuppgifter.[30] Säkerheten ska baseras på:

- Den senaste utvecklingen av tekniskt stöd för säkerhet.
- Kostanden för olika åtgärdsalternativ.
- Risker för den specifika behandlingen.
- Riskernas sannolikhet och allvarsgrad.
- Uppgifternas känslighet.[31]

Generellt sett kan dataskyddets säkerhetskrav sammanställas enligt tabell 1:

[26] Guide to Industrial Control Systems (ICS) Security. NIST Special Publication 800-82 (Revision 2); Kobara, K. (2016). Cyber physical Security for Industrial Control Systems and IOT. *IECE Transactions on Information and Systems 99(4)*; Sagehi, A. R., Wachsmann, C., Waidner, M. (2015). Security and Privacy Challenges in Industrial Internet of Things. *IEEE 2015/2015 52nd ACM/EDAC.*

[27] Eur. Court HR, Niemietz v. Germany judgment of 16 December 1992, Series A no.251-B*;* Eur. Court HR, *Copland v. United Kingdom,* judgment of 3 April 2007, application no. 62617/00; Eur. Court HR*, Halford v. The United Kingdom,* judgment of 25 June 1997, Reports of Judgments and Decisions 1997-III; Eur. Court HR, *Barbulescu v. Romania*, judgment of 5 September 2017, application no. 61496/08; Article 29 Data Protection Working Party. (2017). Opinion 2/2017 on data processing at work. 17/EN WP 249.

[28] Artikel 2, Europaparlamentets och rådets direktiv (EU) 2016/1148 av den 6 juli 2016 om åtgärder för en hög gemensam nivå på säkerhet i nätverks- och informationssystem i hela unionen. OJ L 194.

[29] Artiklarna 5, 32, och 33, förordning (EU) 2016/679.

[30] Datainspektionen. (2008). Säkerhet för personuppgifter. *Datainspektionens allmänna råd.*

[31] Artikel 32, förordning (EU) 2016/679; Datainspektionen. (2008). Säkerhet för personuppgifter. *Datainspektionens allmänna råd.*

Tabell 1. Säkerhetskrav dataskydd.

Styrning	Upprätta lämpliga strategier för dataskydd,[32] instruktioner för anställda som behandlar personuppgifter,[33] samt eventuellt en säkerhetspolicy, om känsliga personuppgifter behandlas, som redovisar strategi, ansvarsfördelning och mål för säkerheten.[34]
Klassning	Upprätta register med bland annat behandlingsändamål, kategorier av registrerade individer, kategorier av behandlade personuppgifter, kategorier av mottagare (även utanför EU), tidsfrister för behandling, och allmän beskrivning av åtgärder.[35]* *Klassning och identifiering sker i samma register i dataskyddet.
Identifiering	
Bedömning	Konsekvensbedömning vid systematiska, omfattande, automatiserade bedömningar (profilering), omfattande behandling av särskilda kategorier av personuppgifter,[36] eller vid systematisk övervakning av allmän plats, inklusive bedömning av risker.[37] Säkerhets-, hot och riskanalyser kan även genomföras.[38]
Åtgärdande	Dokumenterade tekniska och organisatoriska åtgärder.[39]
Incident-hantering	Rapportering av personuppgiftsincidenter.[40]
Revision	Regelbundna tester, undersökningar och utvärderingar av behandlingens säkerhet.[41]

2.3 Informationssäkerhet för samhälls-viktiga och digital tjänster

Direktiv (EU) 2016/1148 (även kallat NIS-direktivet)[42], lag och förordning om informationssäkerhet för samhällsviktiga och digitala tjänster[43] och MSB:s föreskrifter[44] framför krav på säkerhet i nätverk och informationssystem som används för samhällsviktiga tjänster. I denna text refererar vi till samtliga dessa som NIS.

[32] Artikel 24.2, förordning (EU) 2016/679.
[33] Artikel 32.4, förordning (EU) 2016/679.
[34] Datainspektionen. (2008). Säkerhet för personuppgifter. *Datainspektionens allmänna råd.*
[35] Artikel 30, förordning (EU) 2016/679.
[36] Särskilda personuppgifter avser uppgifter personuppgifter om etniskt ursprung, politiska åsikter, religiös eller filosofisk övertygelse eller medlemskap i fackförening, genetik, biometri, hälsa, sexualliv eller sexuella läggning.
[37] Artikel 35, förordning (EU) 2016/679.
[38] Datainspektionen. (2008). Säkerhet för personuppgifter. *Datainspektionens allmänna råd.*
[39] Artiklarna 5, 32, och 33, förordning (EU) 2016/679; Datainspektionen. (2008). Säkerhet för personuppgifter. *Datainspektionens allmänna råd.*
[40] Artikel 33 och 34, förordning (EU) 2016/679.
[41] Artikel 32.1(d), förordning (EU) 2016/679.
[42] Europaparlamentets och rådets direktiv (EU) 2016/1148 av den 6 juli 2016 om åtgärder för en hög gemensam nivå på säkerhet i nätverks- och informationssystem i hela unionen. OJ L 194.
[43] Lag (2018:1174) om informationssäkerhet för samhällsviktiga och digitala tjänster; Förordning (2018:1175) om informationssäkerhet för samhällsviktiga och digitala tjänster.
[44] Myndigheten för samhällsskydd och beredskaps föreskrifter om anmälan och identifiering av leverantörer av samhällsviktiga tjänster. MSBFS 2018:7; Myndigheten för samhällsskydd och beredskaps föreskrifter om informationssäkerhet för leverantörer av samhällsviktiga tjänster. MSBFS 2018:8; Myndigheten för samhällsskydd och beredskaps föreskrifter om rapportering av incidenter för leverantörer av samhällsviktiga tjänster. MSBFS 2018:9; Myndigheten för samhällsskydd och

Inom NIS innebär säkerhet förmågan att motstå åtgärder som underminerar tillgängligheten, riktigheten, integriteten eller konfidentialiteten hos uppgifter eller deras besläktade tjänster. Förmågan avser särskilda nätverks- och informationssystem, bland annat sammankopplade eller sammanhörande enheter som utför automatisk behandling av digitala uppgifter.[45] Att dessa system även kan inbegripa industriella informations- och styrsystem framgår i beskrivningen av nätverks- och informationssystemen och deras användning. För det första att systemen omfattar de digitala uppgifter i sig. Dessutom att enheterna kan vara informationsbehandlande enheter. Därtill att behandlingen kan vara ett led i att driva, använda och skydda, såväl som underhålla enheterna.[46] Slutligen att säkerheten i uppgifterna, enheterna och verksamheten i stort kan ha koppling till fysisk infrastruktur.[47]

Säkerhetskraven gäller inte för alla informations- och styrsystem, men är utformade för att skydda systemen när de används av leverantörer av samhällsviktiga tjänster.[48] De samhällsviktiga tjänsterna omfattar viss verksamhet inom elproduktion och eldistribution, dricksvattendistribution, och spårbunden trafik.[49] Regleringen förhåller sig till aktörer och verksamhet inom dessa sektorer enligt tabell 2:

beredskaps föreskrifter om frivillig rapportering av incidenter i tjänster som är viktiga för samhällets funktionalitet. MSBFS 2018:11.

[45] Artikel 4, Direktiv (EU) 2016/1148.

[46] Artikel 4, Direktiv (EU) 2016/1148.

[47] Skäl 57, Artikel 4, Direktiv (EU) 2016/1148.

[48] Artiklarna 4 och 5, Direktiv (EU) 2016/1148.

[49] Annex II, Europaparlamentets och rådets direktiv (EU) 2016/1148 av den 6 juli 2016 om åtgärder för en hög gemensam nivå på säkerhet i nätverks- och informationssystem i hela unionen. OJ L 194.

Tabell 2. Informationssäkerhet samhällsviktiga och digitala tjänster.

Sektor	NIS-direktivet	MSBFS 2018:7
Elproduktion och eldistribution	Elföretag som bedriver leverans eller handel enligt direktiv 2009/72/EG.[50] Systemansvariga för distributionssystemet enligt direktiv 2009/72/EG.[51]	Elöverföring som tillhandahålls av certifierat transmissionsnätsföretag enligt lag (2011:710).[52] Elöverföring i regionnät enligt EIFS (2012:4)[53] Eldistribution till elanvändare med styrel prioritetsklass 1–5 enligt förordning (2011:931).[54] Elproduktion som är ansluten till stam-, regionnät, eller industri. Elhandel enligt ellagen (1997:857).[55]
Dricksvatten produktion och vattendistribution	Leverantörer och distributörer av dricksvatten enligt direktiv 98/83/EG.[56]	Leveranser av dricksvatten enligt lag (2006:412)[57] som ägaren av den allmänna va-anläggningen tillhandahåller till minst 20 000 personer, eller akutsjukhus.
Spårbunden trafik	Infrastrukturförvaltare av järnvägsinfrastruktur enligt direktiv 2012/34/EU.[58]	Infrastrukturförvaltning eller trafikledning av järnväg på över 200 spårkilometer. Persontrafik på huvudspår där det årliga trafikarbetet överstiger 1 500 000 tågkilometer. Godstrafik på huvudspår där det årliga trafikarbetet överstiger 1 500 000 tågkilometer.
Hälso- och sjukvård	Vårdgivare enligt direktiv 2011/24/EU.[59]	Hälso- och sjukvård som tillhandahålls av vårdgivare enligt hälso- och sjukvårdslag (2017:30)[60], tandvårdslag (1985:125)[61] eller detaljhandel med läkemedel enligt lag (2009:366)[62]

[50] Europaparlamentets och rådets direktiv 2009/72/EG av den 13 juli 2009 om gemensamma regler för den inre marknaden för el och om upphävande av direktiv 2003/54/EG (Text av betydelse för EES). OJ L 211.
[51] Europaparlamentets och rådets direktiv 2009/72/EG av den 13 juli 2009 om gemensamma regler för den inre marknaden för el och om upphävande av direktiv 2003/54/EG (Text av betydelse för EES). OJ L 211.
[52] Lag (2011:710) om certifiering av transmissionsnätsföretag för el. SFS nr: 2011:710.
[53] Energimarknadsinspektionens föreskrifter och allmänna råd om redovisning av nätverksamhet. EIFS 2012:4.
[54] Förordning (2011:931) om planering för prioritering av samhällsviktiga elanvändare.
[55] Ellag (1997:857).
[56] Rådets direktiv 98/83/EG av den 3 november 1998 om kvaliteten på dricksvatten. OJ L 330.
[57] Lag (2006:412) om allmänna vattentjänster.
[58] Europaparlamentets och rådets direktiv 2012/34/EU av den 21 november 2012 om inrättande av ett gemensamt europeiskt järnvägsområde Text av betydelse för. EES OJ L 343.
[59] Europaparlamentets och rådets direktiv 2011/24/EU av den 9 mars 2011 om tillämpningen av patienträttigheter vid gränsöverskridande hälso- och sjukvård. OJ L 88.
[60] Hälso- och sjukvårdslag (2017:30).
[61] Tandvårdslag (1985:125).
[62] Lag (2009:366) om handel med läkemedel.

NIS täcker inte sektorerna för produktion och distribution av fjärrvärme/kyla kemisk processindustri, eller elektroniska kommunikationer.

Leverantörerna av samhällsviktiga tjänster ska vidta lämpliga, ändamålsenliga och proportionella tekniska samt organisatoriska åtgärder för riskerna mot nätverks- och informationssystem.[63] Informationssäkerhetsarbetet ska vara riskbaserat och systematiskt[64] och baserat på standarderna SS-EN ISO/IEC 27001:2017 och SS-EN ISO/IEC 27002:2017 eller motsvarande. Leverantörer ska dessutom tillämpa ett ledningssystem för informationssäkerhet, med en metodik för verksamhetsrisk för att ”införa, driva, övervaka, granska, underhålla och utveckla organisationens informationssäkerhet”.[65] Denna rapport redogör inte för en fullständig kravlista för säkerhet kopplat till NIS men en övergripande analys av kraven kan sammanställas enligt tabell 3:

[63] Artikel 14, Direktiv (EU) 2016/1148; 14§ lag (2018:1174) om informationssäkerhet för samhällsviktiga och digitala tjänster.
[64] 11 till 14 §§, lag (2018:1174) och 7§, förordning (2018:1175) om informationssäkerhet för samhällsviktiga och digitala tjänster.
[65] 4§, Myndigheten för samhällsskydd och beredskaps föreskrifter om informationssäkerhet för leverantörer av samhällsviktiga tjänster. MSBFS 2018:8.

Tabell 3. Kravlista säkerhet kopplat till NIS.

Styrning	Fastställd informationssäkerhetspolicy med målsättningar, inriktning och interna regler för informationssäkerhet, samt ansvarsfördelning.[66]
Klassning	Informationsklassning med utgångspunkt i en konsekvensanalys angående brister i konfidentialitet, riktighet och tillgänglighet.[67]
Identifiering	Identifiering av leverantör av samhällsviktiga tjänster,[68] samt skyddsbehov för olika typer av information enligt informationsklassningsmodellen, (organisatoriska) behov av informationssäkerhet, och eventuella orsaker till incidenter.[69]
Bedömning	Riskanalys, inklusive bedömning av hot och sårbarheter, i enlighet med SS-EN ISO/IEC 27001:2017 avseende organisationens information, nätverk och informationssystem.[70]
Åtgärdande	Åtgärdsplan med tekniska och organisatoriska åtgärder, bland annat enligt MSBFS 2018:8, SS-EN ISO/IEC 27001:2017 och SS-EN ISO/IEC 27002:2017[71]
Incidenthantering	Upptäck, analys och minimera konsekvenserna av incidenter[72] samt rapportering av incidenter med betydande verkan på kontinuiteten i samhällsviktiga tjänster.[73]
Revision	Uppföljning (minst två gånger per år) samt utvärdering av åtgärder och incidenthantering.[74]

[66] 6-8 §§, Myndigheten för samhällsskydd och beredskaps föreskrifter om informationssäkerhet för leverantörer av samhällsviktiga tjänster. MSBFS 2018:8.

[67] 4 och 8 §§, Myndigheten för samhällsskydd och beredskaps föreskrifter om informationssäkerhet för leverantörer av samhällsviktiga tjänster. MSBFS 2018:8.

[68] Myndigheten för samhällsskydd och beredskaps föreskrifter om anmälan och identifiering av leverantörer av samhällsviktiga tjänster. MSBFS 2018:7.

[69] 4, 6, 9, 11, 12 §§, Myndigheten för samhällsskydd och beredskaps föreskrifter om informationssäkerhet för leverantörer av samhällsviktiga tjänster. MSBFS 2018:8.

[70] Artikel 4, Europaparlamentets och rådets direktiv (EU) 2016/1148 av den 6 juli 2016 om åtgärder för en hög gemensam nivå på säkerhet i nätverks- och informationssystem i hela unionen. OJ L 194; 5, 6, 8 §§, Myndigheten för samhällsskydd och beredskaps föreskrifter om informationssäkerhet för leverantörer av samhällsviktiga tjänster. MSBFS 2018:8; 8 § Myndigheten för samhällsskydd och beredskaps allmänna råd om informationssäkerhet för leverantörer av samhällsviktiga tjänster. MSBFS 2018:8.

[71] 5, 8 §§, Myndigheten för samhällsskydd och beredskaps föreskrifter om informationssäkerhet för leverantörer av samhällsviktiga tjänster. MSBFS 2018:8; 8 och 10 §§, Myndigheten för samhällsskydd och beredskaps allmänna råd om informationssäkerhet för leverantörer av samhällsviktiga tjänster. MSBFS 2018:8.

[72] Artikel 4, Direktiv (EU) 2016/1148; 11 §, Myndigheten för samhällsskydd och beredskaps föreskrifter om informationssäkerhet för leverantörer av samhällsviktiga tjänster. MSBFS 2018:8; 6 §, Myndigheten för samhällsskydd och beredskaps allmänna råd om informationssäkerhet för leverantörer av samhällsviktiga tjänster. MSBFS 2018:8.

[73] Artikel 14, Direktiv (EU) 2016/1148; 18 §, lag (2018:1174); 9, 13, 14 §§ förordning (2018:1175); Myndigheten för samhällsskydd och beredskaps föreskrifter om rapportering av incidenter för leverantörer av samhällsviktiga tjänster. MSBFS 2018:9; Myndigheten för samhällsskydd och beredskaps föreskrifter om frivillig rapportering av incidenter i tjänster som är viktiga för samhällets funktionalitet. MSBFS 2018:11.

[74] 6, 8, 9, 12 §§, Myndigheten för samhällsskydd och beredskaps föreskrifter om informationssäkerhet för leverantörer av samhällsviktiga tjänster. MSBFS 2018:8; 6 och 9 §§, Myndigheten för samhällsskydd och beredskaps allmänna råd om informationssäkerhet för leverantörer av samhällsviktiga tjänster. MSBFS 2018:8.

2.4 Informationssäkerhet för myndigheter

Operativ användning av informations- och styrsystem förekommer även inom vissa typer av myndighetsverksamhet. Exempelvis handhar Svenska kraftnät styrsystem för stamnätet,[75] Trafikverket har styrsystem för bland annat broöppning och belysning[76] och Luftfartsverket genomför tester för distansbaserad, automatiserad och intelligent flygledning och flygplatsunderhåll.[77] Det är därför även relevant att beakta informationssäkerhetskrav för myndigheter i enlighet med lag om totalförsvar och höjd beredskap,[78] i fråga om civil verksamhet, samt förordning om krisberedskap och bevakningsansvariga myndigheters åtgärder vid höjd beredskap (krisberedskapsförordningen),[79] och MSB:s föreskrifter om statliga myndigheters informationssäkerhet[80] och statliga myndigheters rapportering av it-incidenter.[81] MSB uppdaterade dessa föreskrifter under september 2020.[82]

I krisberedskapsförordningen fastställs myndigheters ansvar för tillfredsställande säkerhetskrav för egna informationshanteringssystem, inklusive säkra ledningssystem. Detta summeras som ansvar för säker informationshantering, respektive informationssäkerhet i MSB:s föreskrifter. Informationssäkerhet i detta sammanhang avser ”bevarande av konfidentialitet, riktighet och tillgänglighet hos information”.[83]

Informationssäkerhetsarbetet ska vara systematiskt och riskbaserat. Arbetet ska bedrivas genom ett ledningssystem för informationssäkerhet. Informationssäkerhetsarbetet ska även beakta ISO/IEC 27001:2017 och ISO/IEC 27002:2017.

---

[75] Svenska kraftnät. (2019). *Kommentar till medias uppgifter om tillgång till styrsystem.* Från: https://www.svk.se/press-och-nyheter/nyheter/allmanna-nyheter/2019/kommentar-till-medias-uppgifter-om-tillgang-till-styrsystem/ (Besökt 20-09-04); Jonas Olsson. (2019). *Svenska Kraftnät medger säkerhetsbrister.* Från: https://www.svt.se/nyheter/inrikes/svenska-kraftnat-medger-sakerhetsbrister (Besökt 20-09-04).

[76] Radic, J. P., Frank, J. (2018). Projekt för styrsystem för belysning och styrning på distans av bangårdsbelysning. Trafikverket 2018:176; Trafikverket. (2018). *Nytt styrsystem på Kvicksundsbron.* Från: https://www.trafikverket.se/om-oss/nyheter/Lansvisa-nyheter/Vastmanland/2018/nytt-styrsystem-pa-kvicksundsbron/ (Besökt 20-09-04).

[77] Oskar Alex. (2019). *Snart kan robotar sköta flygplatserna.* Från: https://fof.se/artikel/snart-kan-robotar-skota-flygplatserna. Senast 04/09/2020; Johan Eriksson. (2017). *Hur klokt är det att fjärrstyra flygtrafiken?.* Från: https://kuriren.nu/nm4701463. (Besökt 20-09-04).

[78] Lag (1992:1403) om totalförsvar och höjd beredskap i fråga om civil verksamhet.

[79] 19-20 §§ Förordning (2015:1052) om krisberedskap och bevakningsansvariga myndigheters åtgärder vid höjd beredskap.

[80] Myndigheten för samhällsskydd och beredskaps föreskrifter om informationssäkerhet för statliga myndigheter; MSBFS 2020:6 och föreskrifter om säkerhetsåtgärder i informationssystem för statliga myndigheter, MSBFS 2020:7.

[81] Myndigheten för samhällsskydd och beredskaps föreskrifter om rapportering av it-incidenter för statliga myndigheter, MSBFS 2020:8.

[82] Myndigheten för samhällsskydd och beredskap. (2020). Förslag till nya föreskrifter om informationssäkerhet och it-säkerhet för statliga myndigheter. Från: https://www.msb.se/sv/regler/remisser-om-foreskrifter-och-allmanna-rad/tidigare-remisser/forslag-till-nya-foreskrifter-om-informationssakerhet-och-it-sakerhet-for-statliga-myndigheter/ (Besökt 20-09-04).

[83] 1-5 §§, Myndigheten för samhällsskydd och beredskaps föreskrifter informationssäkerhet för statliga myndigheter. MSBFS 2020:6.

Säkerhetskraven utifrån förordningen och föreskrifterna kan sammanställas enligt övergripande kategorier i tabell 4: [84]

Tabell 4. Informationssäkerhet för myndigheter.

Styrning	Fastställd informationssäkerhetspolicy, med målsättningar, inriktning och koppling till interna regler för informationssäkerhetsarbetet.
Klassning	Informationsklassning med fokus på konfidentialitet, riktighet, tillgänglighet och konsekvensnivåer för eventuella skyddsbrister.
Identifiering	Identifiering av risker och behov av säkerhetsåtgärder, gap mellan faktiska åtgärder och åtgärdsbehov, behov av skalskydd, tekniska system mot obehörigt tillträde och fysiskt separerade zoner i lokalerna, grundorsaker till eventuella incidenter och avvikelser, samt behov av kontinuitet vid incident.
Bedömning	Bedöm risker och nivåer av konsekvenser för risker, inklusive vid ackumulering och aggregering av information, bedöm incidenter och avvikelser, inklusive behov av rapportering.
Åtgärdande	Säkerhetsåtgärder, bland annat baserat på ISO/IEC 27001 och ISO/IEC 27002.
Incident-hantering	Åtgärder som säkerställer förmågan att upptäcka, bedöma och rapportera incidenter samt återställa information, och avgöra grundorsaker för incidenter och avvikelser, samt upprätthålla kontinuitet.
Revision	Minst årlig uppföljning av informationssäkerhetsarbetets överenstämmelse med målsättningar, inklusive interna regler, arbetssätt och stöd, samt deras tillämpning, klassningar, riskbedömningar, åtgärder, samt åtgärdernas motsvarighet till behov och hinder för att uppnå mål.

2.5 Säkerhetsskydd

Rapporten *NCS3 – Regelverk och krav inom området industriella informations- och styrsystem (FOI-R--4197--SE)*, uppmärksammade förslaget om en ny säkerhetsskyddslag och dess betydelse för säkerheten i informations- och styrsystem. Sedan rapporten skrevs har säkerhetsskyddslagen, med tillhörande förordning,[85] samt ett antal föreskrifter och vägledningar från Säkerhetspolisen [86] antagits. Offentlighets- och sekretesslagen med tillhörande förordning[87] gäller fortsatt som del av regleringen av sekretess i Sverige även om denna reglering är mindre fokuserad på tekniska system.

[84] 1, 3-6, 10-16 §§, Myndigheten för samhällsskydd och beredskaps föreskrifter om informationssäkerhet för statliga myndigheter, MSBFS 2020:6; Myndigheten för samhällsskydd och beredskaps föreskrifter om säkerhetsåtgärder i informationssystem för statliga myndigheter, MSBFS 2020:7.

[85] Säkerhetsskyddslag (2018:585); säkerhetsskyddsförordning (2018:658).

[86] Säkerhetspolisens föreskrifter om säkerhetsskydd, PMFS 2019:2; Säkerhetspolisen. (2019). Vägledning i säkerhetsskydd: Introduktion till säkerhetsskydd; Säkerhetspolisen. (2019). Vägledning i säkerhetsskydd: Säkerhetsskyddsanalys; Säkerhetspolisen. (2019). Vägledning i säkerhetsskydd: Informationssäkerhet; Säkerhetspolisen. (2019). Vägledning i säkerhetsskydd: Fysisk säkerhet; Säkerhetspolisen. (2019). Vägledning i säkerhetsskydd: Personalsäkerhet; Säkerhetspolisen. (2019). Vägledning i säkerhetsskydd: Säkerhetsskyddad upphandling.

[87] Offentlighets- och sekretesslag (2009:400); offentlighets- och sekretessförordning (2009:641).

Den nya lagen omfattar säkerhetskänslig verksamhet, det vill säga verksamhet med betydelse för Sveriges säkerhet och Sveriges internationella åtagande inom säkerhetsskydd. Lagen omfattar också sekretessbelagda uppgifter som rör den säkerhetskänsliga verksamheten, det vill säga säkerhetsskyddsklassificerade uppgifter. Säkerhetsskyddet avser fortsatt skydd mot spionerі, sabotage, terroristbrott och andra brott samt säkerhetsskyddsklassificerade uppgifter. Regleringen behandlar säkerhet ur tre huvudsakliga perspektiv:[88]

- Informationssäkerhet: åtgärder som förebygger obehörig röjning, ändring, otillgängliggörande av säkerhetsskyddsklassificerade uppgifter och skadlig inverkan på informationssystem i säkerhetskänslig verksamhet.
- Fysisk säkerhet: åtgärder för att förebygga obehörigt tillträde till och skadlig inverkan på områden, byggnader och andra anläggningar eller objekt med säkerhetsskyddsklassificerade uppgifter och säkerhetskänslig verksamhet.
- Personalsäkerhet: kunskapshöjande åtgärder för personal om säkerhetsskyddet samt åtgärder för att förebygga att opålitliga personer deltar i säkerhetskänslig verksamhet och verksamhet med säkerhetsskyddsklassificerade uppgifter.

Som påpekas i den föregående rapporten *(FOI-R--4197--SE)*, motiveras reformerna i säkerhetsskyddet bland annat utifrån behovet av säkra informations- och styrsystem[89] och SCADA (Supervisory Control And Data Acquisition) inom sektorer som vattenförsörjning och transport och kommunikation, exempelvis styrning av järnvägsväxlar. En särskilt uppmärksammad sektor i förslaget om säkerhetsskyddsreformer var elsektorn, detta på grund av samhällets omfattande beroenden av elförsörjning och sektorns beroende av it-system för ” drift, övervakning och styrning”. Förslaget om en ny säkerhetsskyddslag uppmärksammar även förekomsten av samhällsviktiga system inom ”ledningscentraler för trafiksystem, administrativa och medicinska system inom sjukvården, digitala kontrollsystem för el och vatten samt elektroniska kommunikationer”. [90] De sektorer och den verksamhet som omnämns i förslaget och har relevans för denna rapport förtydligas i tabell 5: [91]

[88] 1-4 §§, Säkerhetsskyddslag (2018:585).
[89] Mossberg Sonnek, K, Lindgren F. (2015). NCS3 – Regelverk och krav inom området industriella informations- och styrsystem, FOI-R--4197—SE, s. 11f.
[90] En ny säkerhetsskyddslag. SOU 2015:25, s. 230, 298-301, 398.
[91] En ny säkerhetsskyddslag. SOU 2015:25, s. 298-300.

Tabell 5. Sektorer och verksamheter i förslaget till ny säkerhetsskyddslag.

Sektor	Verksamhet
Elproduktion och distribution	Verksamhet som associeras med kritiska beroenden, inklusive ”system och funktioner som är kritiska för produktion, transmission och distribution av energi”, elhandel, anläggningar, driftsfunktioner, datastöd samt information om ” anläggningars sårbarheter och kapacitet, funktion och roll i elsystemet, exakta lägesangivningar” och skyddsåtgärder.
Dricksvatten-produktion och distribution	Centrala funktioner och system, inklusive informations- och styrsystem, för försörjning och hantering av dricksvatten om ett angrepp mot dessa skulle få ”allvarliga nationella konsekvenser”.
Kemisk processindustri	Industriverksamhet, inklusive forskning och utveckling, som hanterar giftiga material i stor omfattning och annan nationellt viktig produktion.
Spårbunden trafik	System för ”styrning av kritiska järnvägsväxlar”.
Elektronisk kommunikation	Skyddsvärda funktioner såsom ”driftledningscentraler och centrala kopplingspunkter med utrustning för trafikutbyte och signalering, större transmissionsnät samt samverkanspunkter för signalspaning” och system för hemlig avlyssning.
Hälso- och sjukvård	Kritisk verksamhet inom sjukvård, exempelvis som centrala läkemedelslager och laboratorier med smittoämneshantering.

Förslaget om en ny säkerhetsskyddslag behandlade inte vilken verksamhet, vilka system eller funktioner inom produktion av fjärrvärme- och kyla som kan komma att omfattas av säkerhetsskyddet. Däremot övervägdes möjligheten att tilldela Energimyndigheten föreskriftsrätt för denna sektor.[92]

Ansvaret för säkerheten i den verksamhet som regleras av säkerhetsskyddet åligger verksamhetsutövaren. Den operativa utformningen av säkerhetskrav och säkerhetsåtgärder anpassas efter verksamhetens art och behov, exempelvis beroende på typer av skada och konsekvenser samt klassificering av uppgifter. [93] På en övergripande nivå kan säkerhetskraven summeras enligt tabell 6:

[92] En ny säkerhetsskyddslag. SOU 2015:25, s. 492.
[93] Säkerhetsskyddslag (2018:585); Säkerhetsskyddsförordning (2018:658); Säkerhetspolisens föreskrifter om säkerhetsskydd, PMFS 2019:2.

Tabell 6. Säkerhetskrav och säkerhetsåtgärder.

Styrning	Dokumenterade rutiner för behandlingen av säkerhetsskyddsklassificerade uppgifter, handlingar med mera, åtkomst till fysiska och elektroniska nycklar, upprätthållande av kontinuitet i verksamheten, hantering av skadehotande händelser, lagringsmedium, informationssystem, säkerhetsloggning, och säkerhetsövervakning.[94]
Klassning	Säkerhetsuppgiftsklassificering enligt klasserna *kvalificerat hemlig* för synnerlig allvarlig skada vid röjning, *hemlig* för allvarlig skada vid röjning, *konfidentiell* för inte obetydlig skada vid röjning, eller *begränsat hemlig* för ringa skada vid röjning.[95]
Identifiering	Identifiering av säkerhetskänslig verksamhet och skyddsvärden, inklusive säkerhetskänsliga anläggningar, objekt, system, typer av skada och konsekvenser,[96] hot och sårbarheter.[97]
Bedömning	Säkerhetsskyddsanalys där behovet av säkerhetsskydd utreds, inklusive de ovannämnda identifieringsåtgärderna, bedömning av konsekvensnivåer, samt bedömning av säkerhetsskyddsåtgärder mot hot och sårbarheter.[98]
Åtgärdande	Fastställ säkerhetsskyddsplan som klargör vilka säkerhetsskyddsåtgärder som ska vidtas och av vem.[99]
Incident-hantering	Förse informationssystem med funktioner för intrångsdetektering och intrångsskydd[100] samt hantera, minimera och anmäl säkerhetshotande händelser såsom it-incidenter.[101]
Revision	Regelbunden utvärdering, uppföljning och identifiering av brister och sårbarheter i säkerhetsskyddsarbetet samt uppdatering av säkerhetsskyddsanalysen vartannat år.[102]

[94] 1 kap. 5§, 2 kap. 17, 19-20 §§, 3 kap. 3, 27 §§, 4 kap. 10, 32, 37 §§, Säkerhetspolisens föreskrifter om säkerhetsskydd, PMFS 2019:2.
[95] 5 § Säkerhetsskyddslag (2018:585).
[96] Bilaga till Säkerhetsskyddsförordning (2018:658); 2 kap. 1-2 §, Säkerhetspolisens föreskrifter om säkerhetsskydd, PMFS 2019:2.
[97] 2 kap. 7-9 §§, Säkerhetspolisens föreskrifter om säkerhetsskydd, PMFS 2019:2.
[98] 2 kap. 1 § Säkerhetsskyddslag (2018:585); 2 kap. 1 § säkerhetsskyddsförordning (2018:658); 2 kap. Säkerhetspolisens föreskrifter om säkerhetsskydd, PMFS 2019:2.
[99] 2 kap. 1 § Säkerhetsskyddslag (2018:585);2 kap. 11 § Säkerhetspolisens föreskrifter om säkerhetsskydd, PMFS 2019:2.
[100] 4 kap. 29-30 §§, Säkerhetspolisens föreskrifter om säkerhetsskydd, PMFS 2019:2.
[101] 2 kap. 10 § Säkerhetsskyddsförordning (2018:658); 2 kap. 20-26 §§ Säkerhetspolisens föreskrifter om säkerhetsskydd, PMFS 2019:2.
[102] 2 kap. 10, 26 §§, Säkerhetspolisens föreskrifter om säkerhetsskydd, PMFS 2019:2.

3 Elproduktion och eldistribution

3.1 Tillämplig lagstiftning

Elberedskapslagen[103] innehåller bestämmelser om skyldighet att vidta beredskapsåtgärder inom elsektorn och gäller för de som bedriver produktion, handel eller överföring av el. Med beredskapsåtgärder avses enligt lagen åtgärder som behövs för att förebygga, motstå och hantera störningar i elförsörjningen som kan medföra svåra påfrestningar på samhället. Elberedskapsmyndigheten Affärsverket svenska kraftnät (SvK), som pekas ut i elberedskapsförordningen,[104] får meddela föreskrifter om beredskapsåtgärder.

Ellagen[105] innehåller bestämmelser om elektriska anläggningar och om handel med el i vissa fall, men industriella informations- och styrsystem nämns inte specifikt. Däremot finns i lagen ett funktionskrav som säger att avbrott i överföringen av el till elanvändare aldrig får överstiga tjugofyra timmar samt regler om ersättning till de som drabbas av längre avbrott. Detta torde vara ett incitament för nätföretagen att vidta beredskapsåtgärder som minskar risken för driftstörningar. Lagen ställer även krav på årligt upprättande av risk- och sårbarhetsanalys avseende leveranssäkerheten i elnätet, och en åtgärdsplan som visar hur leveranssäkerheten i det egna elnätet ska förbättras. Underlaget ska ges in till nätmyndigheten som i elförordningen[106] pekas ut som Energimarknadsinspektionen (Ei). Nätmyndigheten får meddela föreskrifter om innehållet i underlaget.[107]

I förordning om systemansvaret för el[108] pekas SvK ut som systemansvarig myndighet som ska utöva tillsyn över att ellagen och föreskrifter eller villkor som meddelats i anslutning till lagen följs vad gäller frågor om driftsäkerheten hos det nationella elsystemet. Energimarknadsinspektionen är, i enlighet med ett EU-direktiv,[109] nationell tillsynsmyndighet och får meddela föreskrifter om kontroll, provning, besiktning eller andra krav för att säkerställa driftsäkerheten hos det nationella elsystemet. I säkerhetsskyddsförordningen pekas SvK också ut som tillsynsmyndighet över säkerhetsskyddet när det gäller enskilda verksamhetsutövare som bedriver elförsörjningsverksamhet.[110]

---

[103] 1 och 3 §§ Elberedskapslag (1997:288).
[104] 1§ Förordning (1997:294) om elberedskap.
[105] 3:9a och c Ellagen (1997:857).
[106] Elförordning (2013:208).
[107] Energimarknadsinspektionens föreskrifter och allmänna råd om risk- och sårbarhetsanalyser och åtgärdsplaner avseende leveranssäkerhet i elnäten, EIFS 2013:3.
[108] 1, 2, 2a, 16 d och e §§ Förordning (1994:1806) om systemansvaret för el.
[109] Europaparlamentets och rådets direktiv (EU) 2019/944 av den 5 juni 2019 om gemensamma regler för den inre marknaden för el och om ändring av direktiv 2012/27/EU. Som nationell tillsynsmyndighet fullgör Energimarknadsinspektionen uppgifter som följer av Europaparlamentets och rådets förordning (EU) 2019/943 av den 5 juni 2019 om den inre marknaden för el.
[110] 7 kap. 1 § p. 3 Säkerhetsskyddsförordning (2018:658).

Elsäkerhetslagen och tillhörande förordning[111] innehåller bestämmelser för att främja hög elsäkerhet och minska risker för att el orsakar personskada eller sakskada. Bestämmelserna nämner inte uttryckligen informations- och styrsystem, men kan ändå vara av relevans.

3.2 Övriga regler och bestämmelser

I SvK:s föreskrifter[112] framgår vad som ska anses utgöra beredskapsåtgärder. Som förebyggande åtgärder nämns exempelvis förstärkning av it-säkerhet för styr- och reglersystemets kritiska it-processer såsom bland annat brandvägg, kryptering, virusskydd, avbrottsfri kraft. Som en åtgärd för att motstå störningar nämns exempelvis robusthetshöjande teknisk installation i styrsystem och tillhörande kommunikationsförbindelser.

SvK har också utfärdat föreskrifter om driftsäkerhetsteknisk utformning av produktionsanläggningar[113] som kan ha bäring på industriella informations- och styrsystem, utan att nämna dem specifikt. Dessa föreskrifter ställer krav på viss teknisk dimensionering av produktionsanläggningar för att skapa nödvändiga förutsättningarna för driftsäkerhet i det nationella elsystemet. Kraven avser bland annat störningstålighet vid avvikelser i frekvens och/eller spänning och kommunikation och styrbarhet avseende spänning, effekt och driftstatus. Det finns även krav på att vissa anläggningar ska vara utrustade så att de inom 15 minuter efter att en driftstörning inträffat, och även därefter, kan styras manuellt, antingen genom fjärrkontroll eller genom lokalkontroll.

SvK ger ut tekniska riktlinjer för bland annat dokumentation, fysiskt skydd och elsäkerhet. Där finns en stor mängd riktlinjer som behandlar kontrollanläggningar,[114] med både mer generella standarder och krav på säkerhet såväl som mer specifika krav på bland annat datorer, gränssnittet mellan operatör och utrustning för styrning och övervakning (HMI-system), ändutrustningen i fjärrkontroll- och datainsamlingssystem (Remote Terminal Unit, RTU) och dokumentation av kontrollutrustningar. Det finns även riktlinjer för tele- och datakommunikation som tar upp it-säkerhet.[115]

Byggnader, andra anläggningar och områden som används eller är avsedda för försörjning med energi kan beslutas vara skyddsobjekt enligt skyddslagen.[116] SvK

[111] Elsäkerhetslag (2016:732); Elsäkerhetsförordning (2017:218).
[112] 2 § Affärsverket svenska kraftnäts föreskrifter och allmänna råd om elberedskap, SvKFS 2013:2.
[113] 3 och 7 kap. Affärsverket svenska kraftnäts föreskrifter och allmänna råd om driftsäkerhetsteknisk utformning av produktionsanläggningar, SvKFS 2005:2.
[114] TR02-03-02 Standarder och generella krav, utgåva 5; TR02-03-03Datorer i kontrollanläggning, revision D; TR02-04-02 HMI-system, utgåva 7; TR02-04-03 Fjärrkontroll och RTU:er, utgåva 10; TR02-10-01 Dokumentation kontrollutrustningar, utgåva 5.
[115] TR04-02 Tekniska riktlinjer IT-säkerhet, revision B.
[116] 4§ punkt 5 skyddslag (2010:305).

har ett flertal tekniska riktlinjer som behandlar fysiskt skydd.[117] Som tillsynsmyndighet för elförsörjningens säkerhetsskydd har SvK föreskriftsrätt och utfärdar föreskrifter och allmänna råd om säkerhetsskydd till elförsörjningen.[118]

3.2.1 Kärnteknisk verksamhet

För kärnkraftverken styrs verksamheten av krav som finns i Strålsäkerhetsmyndighetens föreskrifter, vilka i sin tur utgår från lagen och förordningen om kärnteknisk verksamhet.[119] I föreskrifterna om fysiskt skydd[120] framgår att ”[d]atoriserade system av betydelse för anläggningens säkerhet inklusive det fysiska skyddet ska vara skyddade mot obehörig åtkomst och dataintrång”. I myndighetens allmänna råd om tillämpningen av föreskrifterna framgår att kravet avser till exempel processdatorer eller blockdatorer samt system såsom tillträdeskontrollsystem, larmdatorsystem med mera. Det tydliggörs att skyddsåtgärder bör vidtas för att skydda systemen både från obehörig åtkomst, till exempel genom att begränsa tillträdet till lokaler där systemen finns, och från dataintrång, till exempel med brandväggar eller fysisk separation från administrativa datanät. Strålsäkerhetsmyndigheten har ett flertal föreskrifter som berör säkerheten i kärnteknisk verksamhet, men ingen av dem nämner specifikt industriella informations- och styrsystem.[121]

EU:s ministerråd beslutade under 2013 och 2014 om ett nytt strålskyddsdirektiv[122] respektive ett ändrat kärnsäkerhetsdirektiv.[123] Den 1 augusti 2017 ändrades lagen om kärnteknisk verksamhet och vissa av Strålsäkerhetsmyndighetens föreskrifter, för att genomföra det ändrade kärnsäkerhetsdirektivet. Den 1 juni 2018 trädde en ny strålskyddslag med förordning[124] och nya föreskrifter i kraft, som tillsammans innebär ett genomförande av strålskyddsdirektivet. Arbetet pågår med en ny lag

[117] TR09 Fysiskt skydd. I dagsläget (21-01-14) finns 23 stycken.
[118] Affärsverket svenska kraftnäts föreskrifter och allmänna råd om säkerhetsskydd, SvKFS 2019:1.
[119] 10 § lag (1984:3) om kärnteknisk verksamhet, 20 a och 21 §§ förordning (1984:14) om kärnteknisk verksamhet.
[120] 11 § Strålsäkerhetsmyndighetens föreskrifter och allmänna råd om fysiskt skydd av kärntekniska anläggningar (konsoliderad version - ändringar införda t.o.m. SSMFS 2018:14), SSMFS 2008:12.
[121] Strålsäkerhetsmyndighetens föreskrifter och allmänna råd om säkerhet i kärntekniska anläggningar (konsoliderad version - ändringar införda genom SSMFS 2010:3, 2011:3, 2014:3, 2017:1, 2018:12), SSMFS 2008:1; Strålsäkerhetsmyndighetens föreskrifter om beredskap vid kärntekniska anläggningar (konsoliderad version - ändringar införda t.o.m. SSMFS 2018:26), SSMFS 2014:2 samt Strålsäkerhetsmyndighetens föreskrifter och allmänna råd om konstruktion och utförande av kärnkraftsreaktorer, SSMFS 2008:17.
[122] Rådets direktiv 2013/59/ Euratom av den 5 december 2013 om fastställande av grundläggande säkerhetsnormer för skydd mot de faror som uppstår till följd av exponering för joniserande strålning, och om upphävande av direktiven 89/618/Euratom, 90/641/Euratom, 96/29/Euratom, 97/43/Euratom och 2003/122/Euratom.
[123] Rådets direktiv 2014/87/Euratom av den 8 juli 2014 om ändring av direktiv 2009/71/Euratom om upprättande av ett gemenskapsramverk för kärnsäkerhet vid kärntekniska anläggningar.
[124] Strålskyddslag (2018:396), Strålskyddsförordning (2018:506).

och förordning om kärnteknisk verksamhet samt nya föreskrifter som ytterligare tydliggör genomförandet av EU:s kärnsäkerhetsdirektiv.[125]

3.2.2 Vattenkraft

Förutom krav på utformningen av vattenkraftaggregat finns också olika bestämmelser kopplade till dammsäkerhet. Exempelvis finns i lagen om skydd mot olyckor bestämmelser om farlig verksamhet.[126] Även elberedskapslagens[127] krav på att verksamhetsutövare ska genomföra risk- och sårbarhetsanalyser och informera om störningar är till för att öka säkerheten. Vattenkraftanläggningar måste analyseras som en integrerad helhet ur ett säkerhetsperspektiv. Förordning om dammsäkerhet[128] innehåller också relevanta bestämmelser om till exempel säkerhetsledningssystem och rutiner för egenkontroll.

[125] https://www.stralsakerhetsmyndigheten.se/regler/foreskrifter/oversyn-av-vara-foreskrifter/ (besökt 20-05-14). För mer information se även SOU 2019:16 Ny kärntekniklag – med förtydligat ansvar.
[126] 2 kap. 4-5 §§ lag (2003:778) om skydd mot olyckor.
[127] 4, 9a §§ elberedskapslag (1997:288).
[128] Förordning (2014:214) om dammsäkerhet.

4 Dricksvattenproduktion och vattendistribution

4.1 Tillämplig lagstiftning

Inom området vattenförsörjning och avlopp utgör lag och förordning om allmänna vattentjänster[129] grunden för det nationella regelverket. Även miljöbalken[130] och förordning om miljöfarlig verksamhet och hälsoskydd[131] innehåller bestämmelser som är relevanta för området. Vad gäller dricksvattenkvalitet är det i första hand livsmedelslagen[132] och tillhörande förordning[133] som reglerar verksamheten. Livsmedelslagen kompletterar också ett stort antal EU-bestämmelser på området.[134] Livsmedelsverket är ansvarig nationell myndighet med föreskriftsrätt. En länsstyrelse i varje vattendistrikt utgör vattenmyndighet med ansvar för förvaltningen av kvaliteten på vattenmiljön i distriktet.[135]

Byggnader, andra anläggningar och områden som används eller är avsedda för försörjning av vatten kan beslutas vara skyddsobjekt enligt skyddslagen.[136]

4.2 Övriga regler och bestämmelser

Livsmedelsverket har beslutat om ett antal föreskrifter[137] inom dricksvattenområdet. Av särskilt intresse vad gäller industriella informations- och styrsystem är föreskriften om åtgärder mot sabotage och annan skadegörelse riktad mot dricksvattenanläggningar.[138] Föreskriften innehåller krav på att förebygga och avhjälpa skadeverkningar till följd av sabotage eller annan skadegörelse som kan påverka kvaliteten på dricksvatten. Den som producerar dricksvatten ska vidta de åtgärder som behövs för att säkerställa att obehöriga personer inte kan bereda sig tillträde till ett vattenverk samt skydda distributionsanläggningar från obehörig åtkomst.

Specifikt nämns också att den som producerar eller tillhandahåller dricksvatten ska vidta de, administrativa och tekniska, åtgärder som behövs för att säkerställa att

[129] Lag (2006:412) om allmänna vattentjänster och förordning (2007:701) om allmänna vattentjänster.
[130] Miljöbalk (1998:808).
[131] Förordning (1998:899) om miljöfarlig verksamhet och hälsoskydd.
[132] Livsmedelslag (2006:804).
[133] Livsmedelsförordning (2006:813).
[134] Tillkännagivande (2019:716) av de EU-bestämmelser som livsmedelslagen (2006:804) kompletterar.
[135] 5 kap. 14 § miljöbalk (1998:808).
[136] 4§ punkt 5 skyddslag (2010:305).
[137] Exempelvis Livsmedelsverkets föreskrifter om ändring i Livsmedelsverkets föreskrifter (SLVFS 2001:30) om dricksvatten, LIVSFS 2017:2.
[138] LIVSFS 2008:13, Åtgärder mot sabotage och annan skadegörelse riktad mot dricksvattenanläggningar (konsoliderad version - innehåller ändringarna LIVSFS 2013:5).

system för drift och övervakning av dricksvattenproduktion och -distribution skyddas mot obehörig åtkomst. Handlingar av betydelse för driften och övervakningen ska också skyddas mot obehörig åtkomst. En handlingsplan ska också upprättas för hur sabotage och annan skadegörelse riktad mot vattenverk och distributionsanläggningar kan upptäckas och hur skadeverkningar ska avhjälpas. Vägledning för tillämpning av Livsmedelsverkets föreskrifter finns i myndighetens webbaserade verktyg Kontrollwiki.[139] Där framgår att föreskriften gäller åtgärder som syftar till att motverka sabotage och skadegörelse som orsakas av människor och som kan påverka dricksvattnets kvalitet. Dessa åtgärder påverkar dock även leveranssäkerheten i dricksvattenförsörjningen, eftersom det oftast inte går att dra en tydlig gräns mellan åtgärder som görs för att skydda dricksvattenkvaliteten och åtgärder för att skydda den mängd dricksvatten som levereras.

Branschorganisationen Svenskt Vatten har tagit fram konkreta råd och riktlinjer för säkerhetsarbete med fysiskt och tekniskt skydd för dricksvatten som kompletterar Livsmedelsverkets föreskrifter.[140] Organisationen har också tagit fram generella råd och riktlinjer för ansvariga inom dricksvattenproduktion[141] . Bland dessa finns ett avsnitt om säkerhetsanalys som nämner personal- och fysisk säkerhet samt it- och informationssäkerhet. Det finns även ett avsnitt som behandlar krishantering där risk- och sårbarhetsanalys samt beredskaps- och krishanteringsplan nämns. Där hänvisas också till en säkerhetshandbok som innehåller ett helt kapitel om säkerhet i industriella kontrollsystem.[142]

Sedan den 1 januari 2017 finns övergripande nationella mål för alla myndigheter i livsmedelskedjan. Bland annat ska konsumenter garanteras säkra livsmedel, inklusive dricksvatten, och samverkande myndigheter ska ta ett gemensamt ansvar för hela livsmedelskedjan, inklusive beredskap. Med utgångspunkt från de övergripande målen har fyra effektmål fastställts, ett av fokusområdena är säkert dricksvatten. Kontrollplanen riktar sig till chefer och ledare på myndigheter i livsmedelskedjan med ansvar för att planera, genomföra och följa upp kontrollen, men också till företag som vill ha inblick i myndigheternas arbete, liksom till konsumenter och övriga intresserade.[143]

[139] Se det webbaserade verktyget på http://kontrollwiki.livsmedelsverket.se/artikel/361/atgarder-mot-sabotage-och-annan-skadegorelse (besökt 20-05-19).
[140] Svenskt Vatten, Råd och riktlinjer – Fysiskt och tekniskt skydd för dricksvatten, december 2011.
[141] Svenskt Vatten, Sammanställning av råd och riktlinjer för ansvariga inom dricksvattenproduktion, Rapport R1, April 2017.
[142] Svenskt vatten, Säkerhetshandbok för dricksvattenproducenter, Publikation U12, 2012.
[143] Sveriges nationella kontrollplan för livsmedelskedjan 2018-2021, https://www.livsmedelsverket.se/produktion-handel--kontroll/nkp-webben (besökt 20-05-18).

5 Fjärrvärme/-kyla – produktion och distribution

5.1 Tillämplig lagstiftning

Eftersom nästan alla fjärrvärmeverk även producerar el gäller samma föreskrifter för dem som för de aktörer som producerar el. Svenska Kraftnät är dock bara tillsynsmyndighet mot elproduktion, inte mot värmeproduktion.

Fjärrvärmelagen[144] och tillhörande förordning[145] reglerar specifikt området, men handlar främst om att värna fjärrvärmekunders intressen och öka insynen i verksamheten för att bedöma om prissättningen är rimlig. Det görs bland annat genom att fjärrvärmeföretagen ska lämna uppgifter om drift- och affärsförhållanden i verksamheten. Dessa uppgifter ska lämnas till Energimarknadsinspektionen som är tillsynsmyndighet[146] över fjärrvärmeföretagen. Uppgifterna innehåller inget särskilt om industriella informations- och styrsystem, utan tillsynen över produktion och distribution tycks handla om hur verksamheten bedrivs i relation till arbetsmiljö- och miljölagstiftning. Varken lagen eller förordningen ställer några krav på utformning och drift av anläggningarna för produktion eller distribution. Författningarna reglerar inte fjärrkyla.

Fjärrvärmelagen innehåller bestämmelser om avbrytande av distributionen av säkerhetsskäl. Dessa syftar bland annat till att undvika personskada och omfattande sakskada samt för att bidra till god distributionssäkerhet. Om distributionen av fjärrvärme avbrutits utan giltiga skäl ska konsumenten ersättas för skada. Det finns ingen specifik reglering vad gäller längden på avbrott motsvarande den som finns på elområdet.

Arbetsmiljölagen[147] innehåller bestämmelser som är av betydelse för fjärrvärmesektorn. Även jordabalken[148], miljöbalken[149] och brottsbalken[150] innehåller bestämmelser som berör fjärrvärmeverksamhet.

[144] Fjärrvärmelag (2008:263).
[145] Fjärrvärmeförordning (2008:526).
[146] 52 § Fjärrvärmelag (2008:263); 5 § Fjärrvärmeförordning (2008:526); 1 § p. 2 Förordning (2016:742) med instruktion för Energimarknadsinspektionen.
[147] Arbetsmiljölag (1977:1160).
[148] Jordabalk (1970:994).
[149] Miljöbalk (1998:808).
[150] Brottsbalk (1962:700).

5.2 Övriga regler och bestämmelser

Fjärrvärmeanläggningar delas översiktligt in i produktionsdelar, distributionsnät och fjärrvärmecentraler som består av trycksatta anordningar. [151] Arbetsmiljöverket har utfärdat föreskrifter som innehåller specifika regler för sådana anordningar. Föreskrifterna [152] samlar alla krav på hur trycksatta anordningar ska användas och kontrolleras och där framgår bland annat krav på riskbedömning, fortlöpande tillsyn, underhåll och kontroll. Krav på systemkontroll och kunskap om styr- och reglersystem hos vissa kategorier av trycksatta anordningar och säkerhetsutrustning kan ha relevans för industriella informations- och styrsystem.

Branschorganisationen Energiföretagen (tidigare Svensk Fjärrvärme) har gett ut en rapport för att ge stöd angående kravet på riskbedömning. [153] I rapporten nämns inget specifikt om risker och hot specifikt knutna till industriella styr- och informationssystem.

Energiföretagen har även tekniska bestämmelser som utgör branschstandard för fjärrvärme- och fjärrkyledistribution och som bör användas vid planering, upphandling och utförande av fjärrvärme- och fjärrkyledistributionssystem. Dessa omfattar handlingar för komponenter, anvisningar, certifiering och garanti. Däri framgår funktions- och utförandekrav med målsättningen att få god funktion, säkra system och långsiktig hållbarhet. Bestämmelserna baseras, enligt uppgift ”på erfarenhet, standardisering, statistik, provning, forskning och utveckling och utgör fjärrvärmebranschens samlade kunskap och kompetens inom distributionsteknik för fjärrvärme och fjärrkyla”. [154] Ingen av bestämmelserna tar specifikt upp industriella styr- och informationssystem.

[151] Svensk Fjärrvärme, säkerhet i fjärrvärmeanläggningar regler och råd för riskbedömning, Rapport | 2004:2.
[152] Arbetsmiljöverkets föreskrifter om användning och kontroll av trycksatta anordningar (Ändringar införda t.o.m. den 29 mars 2019, AFS 2019:1), AFS 2017:3.
[153] Svensk Fjärrvärme, Säkerhet i fjärrvärmeanläggningar – Regler och råd för riskbedömning, 2004:2.
[154] Från Energiföretagens hemsida https://www.energiforetagen.se/medlemsportalen/listsida/fjarrvarmefragor/fjarrvarmedistribution/tekniska-bestammelser/ (besökt 20-05-19).

6 Kemisk processindustri

6.1 Tillämplig lagstiftning

För sektorn kemisk processindustri utgör lagen om åtgärder för att förebygga och begränsa följderna av allvarliga kemikalieolyckor, med tillhörande förordning,[155] grunden för den nationella regleringen. Dessa benämns, tillsammans med miljöbalken (och till miljöbalken knutna bestämmelser),[156] samt plan- och bygglagen,[157] för Sevesolagstiftningen. Dessa regler syftar till att förebygga och begränsa följderna av allvarliga kemikalieolyckor för människor och miljö och utgår från EU:s så kallade Sevesodirektiv.[158] CLP-förordningen[159] om klassificering, märkning och förpackning av ämnen och blandningar har också relevans för Sevesolagstiftningen. Lagstiftningen medför skyldigheter för både verksamhetsutövare och myndigheter.

Lagstiftning inom området arbetsmiljö ställer även krav på hur verksamheten inom kemisk processindustri ska bedrivas.[160] Vid anläggningar där verksamheten kan innebära fara för att en olycka ska orsaka allvarliga skador på människor eller miljön, såsom inom sektorn kemisk processindustri, finns särskilda regler för farlig verksamhet i lagen och förordningen om skydd mot olyckor.[161] Beroende på vilket ämne som hanteras inom verksamheten kan även lagstiftningen om brandfarliga och explosiva varor vara tillämplig.[162]

6.2 Övriga regler och bestämmelser

Kemisk processindustri berörs av ett antal olika lagstiftningsområden och ett flertal nationella myndigheter utfärdar därmed föreskrifter som är relevanta för sektorn. MSB är central tillsynsmyndighet enligt Sevesolagstiftningen och har utfärdat föreskrifter om åtgärder för att förebygga och begränsa följderna av allvarliga

[155] Lag (1999:381) om åtgärder för att förebygga och begränsa följderna av allvarliga kemikalieolyckor och Förordning (2015:236) om åtgärder för att förebygga och begränsa följderna av allvarliga kemikalieolyckor.
[156] Miljöbalk (1998:808); förordning (1998:899) om miljöfarlig verksamhet och hälsoskydd; miljötillsynsförordning (2011:13) och förordning (1998:901) om verksamhetsutövares egenkontroll.
[157] Plan- och bygglag (2010:900).
[158] Europaparlamentets och rådets direktiv 2012/18/EU av den 4 juli 2012 om åtgärder för att förebygga och begränsa faran för allvarliga olyckshändelser där farliga ämnen ingår och om ändring och senare upphävande av rådets direktiv 96/82/EG.
[159] Europaparlamentets och rådets förordning (EG) nr 1272/2008 av den 16 december 2008 om klassificering, märkning och förpackning av ämnen och blandningar, ändring och upphävande av direktiven 67/548/EEG och 1999/45/EG samt ändring av förordning (EG) nr 1907/2006.
[160] Arbetsmiljölag (1977:1160) och arbetsmiljöförordning (1977:1166).
[161] Lag om skydd mot olyckor (2003:778) och förordning (2003:789) om skydd mot olyckor.
[162] Lag (2010:1011) om brandfarliga och explosiva varor och förordning (2010:1075) om brandfarliga och explosiva varor.

kemikalieolyckor.[163] I och med anpassningen till Sevesodirektivet tillkom i föreskrifterna ett antal bestämmelser om tillsyn av tekniska system samt organisations- och driftsystem som tillämpas vid verksamheten. De ska vara utformade för att medge en planerad och systematisk granskning och särskilt omfatta kontroll av exempelvis åtgärder som vidtagits för att förebygga allvarliga kemikalieolyckor och för att begränsa följderna av sådana olyckor.

[163] 11 § Myndigheten för samhällsskydd och beredskaps föreskrifter om åtgärder för att förebygga och begränsa följderna av allvarliga kemikalieolyckor, MSBFS 2015:8.

7 Spårbunden trafik

7.1 Tillämplig lagstiftning

Lagstiftningen inom sektorn spårbunden trafik kan delas in i järnväg, tunnelbana och spårväg. Inom järnväg finns järnvägslagen med tillhörande förordning[164] som ställer krav på säkerhet. Lagstiftningens säkerhetskrav på järnvägssystem handlar om att förebygga skador och olyckor till följd av verksamheten. Infrastrukturförvaltares och järnvägsföretags verksamhet ska exempelvis omfattas av ett säkerhetsstyrningssystem och övriga säkerhetsbestämmelser som behövs för att trygga en säker verksamhet. Varje delsystem och i dessa ingående komponenter ska, utöver säkerhetskraven, även uppfylla föreskrivna krav om bland annat tillförlitlighet, tillgänglighet, hälsa och miljöskydd.[165] För tunnelbane- och spårvägssystem finns motsvarande säkerhetskrav reglerade i lag och förordning om säkerhet vid tunnelbana och spårväg.[166]

Transportstyrelsen ska övervaka järnvägssystemens säkerhet och får meddela föreskrifter om säkerhet när det gäller bland annat säkerhetsstyrningssystem.[167] Transportstyrelsen är också tillsynsmyndighet för tunnelbana och spårväg.[168] Anläggningar och områden som används eller är avsedda för transporter kan, i likhet med infrastruktur inom andra samhällssektorer, klassas som skyddsobjekt.[169]

7.2 Övriga regler och bestämmelser

Transportstyrelsen har gett ut föreskrifter som innehåller bestämmelser om säkerhetsstyrningssystem och övriga säkerhetsbestämmelser enligt järnvägslagen.[170] För tunnelbana och spårväg har Transportstyrelsen gett ut motsvarande föreskrifter som innehåller bestämmelser om säkerhetsstyrning och säkerhetsordning med säkerhetsbestämmelser för spårinnehavare och trafikutövare enligt lagen om säkerhet vid tunnelbana och spårväg.[171] Ingen av nämnda föreskrifter innehåller dock några uttryckliga hänvisningar till informations- och styrsystem.

---

[164] Järnvägslag (2004:519) och järnvägsförordning (2004:526).
[165] 2 kap. 5, 8 §§ järnvägslag (2004:519).
[166] Lag (1990:1157) om säkerhet vid tunnelbana och spårväg och förordning (1990:1165) om säkerhet vid tunnelbana och spårväg.
[167] 2 kap. 1§ järnvägsförordning (2004:526).
[168] 2§ förordning (1990:1165) om säkerhet vid tunnelbana och spårväg.
[169] 4§ punkt 5 skyddslag (2010:305).
[170] Transportstyrelsens föreskrifter om säkerhetsstyrningssystem och övriga säkerhetsbestämmelser för infrastrukturförvaltare med säkerhetstillstånd samt järnvägsföretag med säkerhetsintyg, TSFS 2015:34.
[171] Transportstyrelsens föreskrifter om säkerhetsstyrning och säkerhetsordning med säkerhetsbestämmelser inom tunnelbana och spårväg, TSFS 2013:44.

Järnvägsstyrelsens trafikföreskrifter (JvSFS 2008:7) om signaler och signalsystem upphörde att gälla den 1 mars 2016 och nya föreskrifterna har tagits fram utifrån gällande europeiskt och nationellt regelverk.[172]

Ett antal EU-direktiv och förordningar reglerar de delar av järnvägsnätet som sitter ihop med det europeiska järnvägsnätet och avser att underlätta för järnvägstrafik att passera landsgränser. Exempel på dessa är driftkompabilitetsdirektivet[173], direktivet om säkerhet på gemensamma järnvägar[174] och kommissionens förordning om en gemensam säkerhetsmetod (CSM-RA)[175].

[172] Transportstyrelsens föreskrifter om bedrivande av tågtrafik, TSFS 2015:77, innehåller bestämmelser om bedrivande av tågtrafik som följer av bilagan till kommissionens beslut 2012/757/EU av den 14 november 2012 om teknisk specifikation för driftskompatibilitet avseende delsystemet ”Drift och trafikledning” i järnvägssystemet i Europeiska unionen och om ändring av beslut 2007/756/EG, i lydelse enligt kommissionens beslut 2013/710/EU.

[173] Europaparlamentets och rådets direktiv 2008/57/EG.

[174] Europarådets och parlamentets direktiv 2004/49/EG.

[175] Kommissionens genomförandeförordning (EU) nr 402/2013 av den 30 april 2013 om den gemensamma säkerhetsmetoden för riskvärdering och riskbedömning och om upphävande av förordning (EG) nr 352/2009.

8 Elektroniska kommunikationer

8.1 Tillämplig lagstiftning

Antagandet av Europaparlamentets och rådets direktiv 2002/21/EG[176] innebar en harmonisering av regleringen för elektroniska kommunikationstjänster, elektroniska kommunikationsnät, tillhörande faciliteter och tillhörande tjänster.[177] I praktiken omfattar den väsentliga regleringen för denna rapport två huvudsakliga typer av elektroniska kommunikationer; elektroniska kommunikationer generellt och radiobaserade elektroniska kommunikationer.

8.1.1 Elektroniska kommunikationer generellt

Den övergripande regleringen för elektronisk kommunikation fastställs i direktiv 2002/21/EG, samt direktiv 2002/58/EG (ePrivacy-direktivet)[178] avseende integritetsskydd, och tillämpas i Sverige genom lag och förordning om elektronisk kommunikation,[179] samt Post- och telestyrelsens föreskrifter på området.[180]

Regleringen för elektronisk kommunikation omfattar teknik (och tjänster) såsom:[181]

- **Elektroniska kommunikationsnät:** system och utrustning för överföring av ”signaler via tråd, via radio, på optisk väg eller via andra elektromagnetiska överföringsmedier, däribland satellitnät, fasta nät (kretskopplade och paketkopplade, inbegripet Internet) och markbundna mobilnät, elnätsystem i den utsträckning dessa används för signalöverföring, rundradionät samt kabel-tv-nät, oberoende av vilken typ av information som överförs”.
- **Allmänna kommunikationsnät:** elektroniska kommunikationsnät för allmänt tillgängliga kommunikationstjänster i huvudsak.
- **Elektroniska kommunikationstjänster:** en tjänst för överföring av signaler i elektroniska kommunikationsnät. Ofta tillhandahålls dessa mot ersättning.

[176] Europaparlamentets och rådets direktiv 2002/21/EG av den 7 mars 2002 om ett gemensamt regelverk för elektroniska kommunikationsnät och kommunikationstjänster (ramdirektiv). EGT L 108, 24.4.2002.
[177] Artikel 1, direktiv 2002/21/EG.
[178] Europaparlamentets och rådets direktiv 2002/58/EG av den 12 juli 2002 om behandling av personuppgifter och integritetsskydd inom sektorn för elektronisk kommunikation (direktiv om integritet och elektronisk kommunikation). EGT L 201, 31.7.2002.
[179] Lag (2003:389) om elektronisk kommunikation; Förordning (2003:396) om elektronisk kommunikation.
[180] Register över författningar utfärdade av Post och telestyrelsen, PTSFS 1992–2019.
[181] Artikel 2, direktiv 2002/21/EG; 1 kap, 7§ Lag (2003:389) om elektronisk kommunikation.

- **Kommunikationer:** information som överförs via allmänt tillgängliga kommunikationstjänster mellan ett begränsat antal parter.
- **Elektronisk post:** meddelanden via allmänt tillgängliga kommunikationstjänster som lagras i en mottagares terminalutrustning.
- **Trafikuppgifter:** uppgifter som behandlas för att kunna överföra kommunikationer via ett kommunikationsnät.
- **Lokaliseringsuppgifter:** uppgifter som visar geografisk position för terminalutrustning och behandlas via elektroniska kommunikationsnät.
- **Samtal:** telefonitjänstförbindelser för tvåvägskommunikation.
- **Nödsamtal:** samtal till alarmeringstjänst (112).

Regleringens allmänna mål och principer syftar bland annat till att till att säkerställa de allmänna kommunikationsnätens integritet och säkerhet.[182] Detta innebär att den som tillhandahåller allmänna kommunikationsnät och elektroniska kommunikationstjänster ska vidta lämpliga tekniska och organisatoriska åtgärder för driftsäkerhet,[183] säkerhet vid extraordinära händelser i fredstid[184] samt integritet.[185]

Driftsäkerhet

Åtgärderna ska väljas med beaktande av risk för störningar och avbrott, tillgänglig teknik och genomförandekostnader. Ytterligare krav för driftsäkerhet är fastställda i Post- och telestyrelsens föreskrifter om driftsäkerhet.[186] Arbetet med driftsäkerhet ska vara systematiskt, långsiktigt och bedrivas kontinuerligt med beaktande av normala såväl som extraordinära händelser.[187] Kraven för driftsäkerhet kan bland annat summeras som följer i tabell 7:

[182] Artikel 8, direktiv 2002/21/EG.
[183] 5 kap. 6 b §, Lag (2003:389) om elektronisk kommunikation.
[184] Post- och telestyrelsens allmänna råd om god funktion och teknisk säkerhet samt uthållighet och tillgänglighet vid extraordinära händelser i fredstid. PTSFS 2007:2.
[185] Post- och telestyrelsens föreskrifter och allmänna råd om skyddsåtgärder för behandlade uppgifter. PTSFS 2014:1.
[186] Post- och telestyrelsens föreskrifter om krav på driftsäkerhet. PTSFS 2015:2; Föreskrifter om ändring i Post- och telestyrelsens föreskrifter (PTSFS 2015:2) om krav på driftsäkerhet. PTSFS 2020:1.
[187] 3 §, Post- och telestyrelsens föreskrifter om krav på driftsäkerhet. PTSFS 2015:2.

Tabell 7. Krav driftsäkerhet.

Styrning	Ta fram och dokumentera processer, planer, åtgärder och teser.[188]
Klassning	Samtliga tillgångar och förbindelser, deras funktionalitet, tillverkare, geografiska placering och deras klass baserat på antal anslutningar.[189]
Identifiering	Årlig risk- och konsekvensbedömning för tillgångar och planerade förändringar som kan påverka driftsäkerhet, inklusive identifiering av hot, deras konsekvenser och sannolikhet. Analyserna ska även genomföras vid upphandling.[190] Även konsekvenser av att kritiska verksamhetsdelar helt eller delvis upphör och tillämpningen av särskilda handlingsplaner för sådana situationer ska analyseras.[191]* * Krav för identifiering och bedömning överensstämmer
Bedömning	
Åtgärdande	Fastställd plan för hantering av händelser som kan orsaka störningar eller avbrott samt vidta åtgärder enligt riskbedömningen och de hot som regleras av föreskrifterna såsom väder och intrång.[192]
Incident-hantering	Rapportera och hantera incidenter, samt när det bestämts av tillsynsmyndigheten, informera allmänheten om störningar. [193]
Revision	Revidera konsekvensanalys och särskilda handlingsplaner för upphörandet av kritiska verksamhetsdelar vid behov.[194]

Säkerhet vid extraordinära händelser

Föreskrifter med jämförbara krav på ett systematiskt och kontinuerligt säkerhetsarbete för teknisk säkerhet, uthållighet och tillgänglighet vid extraordinära händelser i fredstid har också utarbetats av Post- och telestyrelsen.[195] Följande tabell 8 redogör för relevanta delar av föreskriftens innehåll:

[188] 3 §, Post- och telestyrelsens föreskrifter om krav på driftsäkerhet. PTSFS 2015:2.
[189] 4, 15 §§, Post- och telestyrelsens föreskrifter om krav på driftsäkerhet. PTSFS 2015:2; 4 §, Föreskrifter om ändring i Post- och telestyrelsens föreskrifter (PTSFS 2015:2) om krav på driftsäkerhet, PTSFS 2020:1.
[190] 5 §, Post- och telestyrelsens föreskrifter om krav på driftsäkerhet. PTSFS 2015:2; 5 och 5 a §, Föreskrifter om ändring i Post- och telestyrelsens föreskrifter (PTSFS 2015:2) om krav på driftsäkerhet, PTSFS 2020:1.
[191] 6 §, Post- och telestyrelsens föreskrifter om krav på driftsäkerhet, PTSFS 2015:2.
[192] 7-14 §§, Post- och telestyrelsens föreskrifter om krav på driftsäkerhet. PTSFS 2015:2; 9-13 §§, Föreskrifter om ändring i Post- och telestyrelsens föreskrifter (PTSFS 2015:2) om krav på driftsäkerhet, PTSFS 2020:1.
[193] 5 kap. Lag (2003:389) om elektronisk kommunikation; 7 §, Post- och telestyrelsens föreskrifter om krav på driftsäkerhet, PTSFS 2015:2.
[194] 6, 8 §§, Post- och telestyrelsens föreskrifter om krav på driftsäkerhet, PTSFS 2015:2.
[195] Post- och telestyrelsens allmänna råd om god funktion och teknisk säkerhet samt uthållighet och tillgänglighet vid extraordinära händelser i fredstid, PTSFS 2007:2.

Tabell 8. Säkerhet vid extraordinära händelser.

Styrning	Dokumenterade rutiner, handlingsplaner.
Identifiering	Regelbundna riskanalyser, inklusive identifiering av områden, hot, och hotens konsekvenser och sannolikheter, samt bedömning av hur hoten ska hanteras.
Bedömning	
Åtgärdande	Upprätta rutiner och handlingsplaner i syfte att vidta skyddsåtgärder för att förebygga, begränsa och hantera störningar och avbrott.
Incident-hantering	Rutiner och handlingsplaner bör bland annat fastställa rutiner för effektivt avhjälpande av avbrott och störningar, organisation för åtgärdande, prioriteringar för åtgärder återställande till normal verksamhetsdrift, extra resurser vid avbrott och störningar, identifiering av störningsorsaker, samt vidarerapportering avseende störningar.
Revision	Följ upp inträffade avbrott och störningar.

Integritet

ePrivacy-direktivet och lag om elektronisk kommunikation inbegriper ett antal säkerhetskrav för elektroniska kommunikationer som främjar integritetsskydd. Bland annat ska leverantörer av allmänt tillgängliga kommunikationstjänster säkerställa lämpliga tekniska och organisatoriska åtgärder för nätsäkerhet. Åtgärderna ska beakta föreliggande risker, teknik och genomförandekostnader.[196] ePrivacy-direktivet och lag om elektronisk kommunikation medför även transparenskrav mot abonnenter. De ska informeras om risker för brott mot nätsäkerheten, åtgärder och åtgärdandekostnader för dessa risker.[197] Kommunikationers konfidentialitet ska även säkerställas på nationell nivå, bland annat med rättsliga åtgärder mot avlyssning, uppfångande, och annan övervakning, annat än vad som tillåts genom lag eller samtycke baserat på tydlig och fullständig information till abonnenten.[198] Dessutom innehåller ePrivacy-direktivet och lagen om elektronisk kommunikation ett antal integritetsrelaterade krav, såsom:[199]

- Skydd av lagrade uppgifter vid behandling.
- Utplåning eller avidentifiering av trafikuppgifter efter att de uppfyllt sitt syfte.
- Abonnenters möjlighet att återkalla samtycke för vissa trafikuppgifter.
- Information till abonnenten om typer av trafikuppgifter som behandlas.
- Begränsad behandling av trafikuppgifter.
- Möjligheten att förhindra nummerpresentation.
- Säkerställande av avidentifiering eller samtycke (som kan återkallas) samt begräsning vid behandling av lokaliseringsuppgifter.

[196] Artikel 4, Direktiv 2002/58/EG; 6 kap. 3§, Lag (2003:389) om elektronisk kommunikation.
[197] Artikel 4, Direktiv 2002/58/EG; 5 kap. 15 §, 6 kap. 4 § Lag (2003:389) om elektronisk kommunikation.
[198] Artikel 5, Direktiv 2002/58/EG; 6 kap. 17-23 §§ Lag (2003:389) om elektronisk kommunikation.
[199] Artikel 6, 8-9, 12-13, Direktiv 2002/58/EG; 5 kap. 15 och 17 a §§, 6 kap. 3 a, 4a-b, 5-7, 9, 16 §§ Lag (2003:389) om elektronisk kommunikation.

- Möjligheten att kontrollera, rätta eller återkalla personuppgifter från abonnentförteckningar.
- Säkerställa samtycke samt andra åtgärder avseende icke begärd kommunikation, såsom direkt marknadsföring.
- Föra förteckning på integritetsincidenter.
- Underrätta tillsynsmyndigheten, samt eventuellt abonnenter, vid integritetsincidenter.

Även i fråga om skyddsåtgärder för behandlade personuppgifter ska den som tillhandahåller elektroniska kommunikationstjänster bedriva ett kontinuerligt och systematiskt säkerhetsarbete med långsiktigt perspektiv. Arbetet ska följa vedertagna normer, standarder och praxis. En övergripande summering av föreskrifterna på detta område framställs i tabell 9:[200]

Tabell 9.Skyddsåtgärder integritet.

Styrning	Dokumenterade rutiner, processer och roller.
Identifiering	Identifiering av informationstillgångar.
Bedömning	Riskanalys för identifierade informationstillgångar.
Åtgärdande	Vidta lämpliga skyddsåtgärder såsom åtkomst- och behörighetshantering, loggningar av behandling, skydd mot utplåning och förlust, och kryptering.
Incident-hantering	Rutiner för identifiering, rapportering och hantering av integritetsincidenter samt förteckning av integritetsincidenter.
Revision	Uppföljning av åtkomstbehörigheter och integritetsincidenter.

8.1.2 Radiokommunikationer

Regleringen av radiokommunikation utgår ifrån direktiv 2002/21/EG, direktiv 2014/53/E (även kallat ”Radio Equipment Directive” – RED), radioutrustningslagen med tillhörande förordning,[201] samt Post- och telestyrelsens föreskrifter för radioutrustning.[202]

Direktiv 2002/21/EG reglerar inte sådan utrustning på radiokommunikationsområdet som omfattas av RED. Istället avser direktiv 2002/21/EG vissa typer av konsumentutrustning där kommunikationsnätssignaler överförs genom radio.[203] Tillhandahållandet och ibruktagandet av radioutrustning regleras av RED samt radioutrustningslag- och förordning. I Sverige regleras radioanvändning utav lag om elektronisk kommunikation.[204] Teknik som regleras på detta område omfattar bland annat radioutrustning och elektriska och elektroniska sändare och mottagare

[200] 3-11 §§, Post- och telestyrelsens föreskrifter och allmänna råd om skyddsåtgärder för behandlade uppgifter, PTSFS 2014:1.
[201] Radioutrustningslag (2016:392); Radioutrustningsförordning (2016:394).
[202] Post- och telestyrelsen föreskrifter om krav m.m. på radioutrustning, PTSFS 2016:5.
[203] Artikel 2, Skäl 8, Direktiv 2002/21/EG.
[204] 1 kap. 4 §, Lag (2003:389) om elektronisk kommunikation.

av radiovågor för radiokommunikation. Den omfattar även radiovågor med frekvenser på 3 000 GHz, samt radiokommunikation med hjälp av sådana radiovågor.[205]

Säkerhetskraven för radioutrustning baseras främst på bestämmelser för att:

- Skydda människors och husdjurs liv, hälsa och säkerhet.
- Skydda egendom.
- Förebygga skador och försämringar på nätet.
- Undvika skadliga störningar.[206]

Skadliga störningar i det här sammanhanget är oönskade utstrålade radiovågor med negativa konsekvenser för radiospektrumpolitikens mål på EU-nivå.[207] På nationell nivå avser det störningar som äventyrar funktionalitet eller ”allvarligt försämrar, hindrar eller upprepat avbryter” radiokommunikationstjänster.[208]

Lagen syftar till att förebygga ovannämnda störningar och skador. Bland annat ska tillstånd med villkor för radioanvändning säkerställa att radiofrekvenser inte riskerar att generera störningarna och innefatta villkor för att skydda liv och hälsa. Tillståndshavare är dessutom skyldiga att se till att eventuella störningar upphör omedelbart när de uppkommer.[209]

Ytterligare krav för tillverkare, tillverkares representanter, importörer, och distributörer av radioutrustning fastställs i Post- och telestyrelsens föreskrifter. Kraven i föreskrifterna innebär bland annat att tillverkare ska tillgodose:

- Information om hur radioutrustning kan användas på ett säkert sätt.
- Skyddsåtgärder mot risker som orsakas av radioutrustningen.
- Skyddsåtgärder mot risker orsakade av yttre påverkan på radioutrustningen. [210]

8.2 Övriga regler och bestämmelser

8.2.1 Förhållande till NIS

NIS-direktivet (direktiv (EU) 2016/1148) sammanfaller till viss del med ePrivacy-direktivet (direktiv 2002/58/EC) när det gäller reglerad teknik. Detta beror på att NIS-direktivets definition för nätverks- och informationssystem omfattar de

[205] Artikel 2, Direktiv 2014/53/EU; 3 §, Radioutrustningslag (2016:392).
[206] Artiklarna 3 och 7, Direktiv 2014/53/E; 3 kap. 11 §, Lag (2003:389) om elektronisk kommunikation.
[207] Skäl 10, Direktiv 2014/53/EU.
[208] 1 kap. 7 §, Lag (2003:389) om elektronisk kommunikation; 3 §, Radioutrustningslag (2016:392).
[209] 3 kap. 6, 11, 13 §§, Lag (2003:389) om elektronisk kommunikation.
[210] 2-4, 8 §§, Radioutrustningsförordning (2016:394).

elektroniska kommunikationsnät som regleras av artikel 2 i ePrivacy-direktivet.[211] På samma sätt är det möjligt att internetbaserade marknadsplatser, såsom de definieras av NIS-direktivet, även använder sig av cookies och liknande och därmed kan behöva tillämpa krav från såväl ePrivacy-direktivet och NIS som Kommissionens tillämpningsföreskrifter för digitala tjänster enligt NIS.[212]

8.2.2 Förhållande till europeisk rymdrättslig reglering

Direktiv 2002/21/EG, ePrivacy-direktivet och NIS-direktivet har samma definition för elektroniska kommunikationsnät där överföring via satellitnät ingår.[213] På rymdarenan bör det även nämnas att det europeiska rymdsamarbetet regleras av ESA-Konventionen.[214] I *Cybersäkerhet på rymdarenan (FOI-D--0820--SE)*[215] uppmärksammas bland annat mötespunkterna mellan rymdrätt och cyberrättslig reglering i stort. Rapporten lyfter exempelvis ESA-konventionens reglering och skyddet av teknisk data, rymdsystemens konstruktion och tillförlitlighetsbedömningar för rymdsystem. För att skydda rymdsystemen har ESA dessutom antagit en säkerhetsförordning[216] och regler för, bland annat, informationshantering.[217] Säkerhetsförordningen reglerar bland annat skydd mot säkerhetsincidenter medan reglerna för informationshantering avser immateriella rättigheter och likande.

[211] Artikel 4, Direktiv (EU) 2016/1148.
[212] Kommissionens genomförandeförordning (EU) 2018/151 av den 30 januari 2018 om tillämpningsföreskrifter för Europaparlamentets och rådets direktiv (EU) 2016/1148 om åtgärder för en hög gemensam nivå på säkerhet i nätverks- och informationssystem i hela unionen vad gäller närmare specificering av de aspekter som ska beaktas av leverantörer av digitala tjänster när de hanterar risker som hotar säkerheten i deras nät- och informationssystem samt parametrarna för fastställande av om en incident har avsevärd inverkan. C/2018/0471. EUT L 26, 31.1.2018.
[213] Artikel 2, Direktiv 2002/21/EG; Artikel 2, Direktiv 2002/58/EG; Artikel 4, Direktiv (EU) 2016/1148.
[214] Convention for the establishment of a European Space Agency (CSE/CS(73)19, rev.7).
[215] Jonatan Westman, Erik Zouave, Christian Valassi. (2017). Cybersäkerhet på rymdarenan: Avskannande projekt 2017. FOI-D--0820--SE.
[216] Regulations of the European Space Agency: Security Regulations ESA/REG/004, rev.1.
[217] Regulations of the European Space Agency: Rules on information, Data and Intellectual Property Rights ESA/REG/008.

9 Hälso- och sjukvård

9.1 Tillämplig lagstiftning

Användningen av informations- och styrsystem i hälso- och sjukvården är både varierad och omfattande. I *NCS3: Informations- och styrsystem inom hälso- och sjukvård (FOI-R--4088--SE)* observerar Holm och Westring att över 20 000 medicintekniska produkter identifierats.[218] I Holms och Westrings rapport går det att läs mer ingående om informations- och styrsystem, incidenter och deras inverkan på patientsäkerhet.

Patientsäkerhetsarbetet utgör grunden för teknisk säkerhet i hälso- och sjukvård. Patientsäkerhet regleras av hälso- och sjukvårdslagen med tillhörande förordning,[219] patientsäkerhetslagen med tillhörande förordning[220] och patientdatalagen[221] med tillhörande förordning. I regleringen av patientdata återfinns dessutom grunden för patienternas integritet i mån av tillämpat personuppgiftsskydd inom vården. Medicinteknik regleras dessutom särskilt utifrån förordning (EU) 2017/745,[222] förordning (EU) 2017/746[223] och lag och förordning om medicintekniska produkter.[224] Dessutom gäller Läkemedelsverkets föreskrifter för sjukvårdsutrustning och dess tillverkning, samt Socialstyrelsens föreskrifter för vård som bedrivs med teknisk utrustning.[225]

9.1.1 God vård

En utgångspunkt för säkerhet i sjukvården är kravet på god vård i hälso- och sjukvårdslagen. Kravet på god vård innebär att hälso- och sjukvårdsverksamhet ska tillgodose patienternas behov av säkerhet och att det ska finnas utrustning som tillgodoser patientens säkerhet.[226] I huvudsak avser säkerheten skydd mot

[218] Holm, H. Westring, E. (2015). NCS3: Informations- och styrsystem inom hälso- och sjukvård (FOI-R--4088--SE).
[219] Hälso- och sjukvårdslag (2017:30); Hälso- och sjukvårdsförordning (2017:80).
[220] Patientsäkerhetslag (2010:659); Patientsäkerhetsförordning (2010:1369).
[221] Patientdatalag (2008:355); Patientdataförordning (2008:360).
[222] Europaparlamentets och rådets förordning (EU) 2017/745 av den 5 april 2017 om medicintekniska produkter, om ändring av direktiv 2001/83/EG, förordning (EG) nr 178/2002 och förordning (EG) nr 1223/2009 och om upphävande av rådets direktiv 90/385/EEG och 93/42/EEG (Text av betydelse för EES.). EUT L 117S.
[223] Europaparlamentets och rådets förordning (EU) 2017/746 av den 5 april 2017 om medicintekniska produkter för in vitro-diagnostik och om upphävande av direktiv 98/79/EG och kommissionens beslut 2010/227/EU (Text av betydelse för EES.). EUT L 117, 5.5.2017.
[224] Lag (1993:584) om medicintekniska produkter; Förordning (1993:876) om medicintekniska produkter.
[225] Patientlag. SOU 2013:2, s. 339.
[226] 5 kap. 1§ Hälso- och sjukvårdslag (2017:30).

patientskador,[227] men det inbegriper även respekt för patienternas integritet.[228] Utrustningen, såsom den tekniska sjukvårdsutrustning och de it-system som används i vården, regleras också av kravet på god vård. [229]

9.1.2 Patientsäkerhet

Arbetet med att säkerställa god vård innebär att vårdgivare ska bedriva ett systematiskt patientsäkerhetsarbete. Patientsäkerhetsarbetet syftar ytterst till att förebygga dödsfall, skador och lidande inom hälso- och sjukvården; så kallade vårdskador. Det innebär bland annat att vårdgivare ska vidta åtgärder för att förebygga och utreda vårdskador.[230] Att arbete med teknisk säkerhet är en del av patientsäkerhet förklaras i redogörelsen av patientsäkerhetsbegreppet i SOU 2008:1177:

> Det finns stora likheter i hur organisationer världen över arbetar med att utveckla och förbättra kvalitet och säkerhet i vården. Säkerhetsarbete i allmänhet och i vården i synnerhet baseras på kunskap från ett flertal ämnesområden bl.a. kunskap om människans fysiska och kognitiva funktioner samt hur teknik och organisation bör utformas med hänsyn till dessa funktioner. I arbetsmiljösammanhang är kraven att arbetsmiljön ska anpassas till människans fysiska, psykologiska och sociala förutsättningar. Det finns krav på att verktyg, maskiner, utrustning av olika slag, arbetsställningar, fysisk miljö etc. ska utformas så att ohälsa och olycksfall förebyggs.[231]

Det systematiska patientsäkerhetsarbetet ska, likt flera delar av den sektorsövergripande regleringen, bedrivas genom ett ledningssystem för verksamheten. Ledningssystemet förhåller sig inte uttryckligen till informations- och styrsystem, men ska byggas upp utifrån standarder, tekniska specifikationer och modeller generellt. Det ska bland annat förebygga och utreda ”brister i samspelet mellan människa, teknik och organisation”. Ledningssystemet ska fastställa principer för verksamheten med patientsäkerhet [232] samt vidta ett antal åtgärder enligt patientsäkerhetslagen och förordningen, SOSFS 2011:9 och HSLF-FS 2017:40. Åtgärdskraven i dessa källor kan summeras i följande huvuddrag:

- Upprätta processer och rutiner.
- Identifiera behov av samverkan för verksamhetskvalitet.
- Genomföra riskanalys.

---

[227] 2 kap. 1§ Hälso- och sjukvårdslag (2017:30); Socialstyrelsen. (2020). *En god och säker vård.* https://patientsakerhet.socialstyrelsen.se/ledning-och-styrning/nationell-handlingsplan/en-god-och-saker-vard/ (Besökt 20-09-17).

[228] 5 kap. 3§ Hälso- och sjukvårdslag (2017:30); Prop. 2016/17:43 En ny hälso- och sjukvårdslag, s.72; SOU 2013:2 Patientlag s. 53, 308-309.

[229] SOU 2013:2 Patientlag s. 339.

[230] 3 kap, Patientsäkerhetslag (2010:659); Socialstyrelsens föreskrifter och allmänna råd om vårdgivares systematiska patientsäkerhetsarbete. HSLF-FS 2017:40.

[231] SOU 2008:1177 Patientsäkerhet: Vad har gjorts? Vad behöver göras?, s. 92.

[232] 2 kap. 1§, 3 Kap. 1§ och 4 kap. 1§ Socialstyrelsens föreskrifter och allmänna råd om ledningssystem för systematiskt kvalitetsarbete, SOSFS 2011:9 och HSLF-FS 2017:40.

- Utöva egenkontroll.
- Utreda avvikelser.
- Genomföra förbättringsarbete.
- Dokumentera.[233]

9.1.3 Patientdata

Specialbestämmelser för skyddet av patienters integritet i hälso- och sjukvården finns i patientdatalagen med tillhörande förordning[234] samt Socialstyrelsens föreskrifter för journalföring och behandling av personuppgifter.[235] Utöver integritetsskydd syftar bestämmelserna även till att säkerställa patientsäkerhet vid behandling av personuppgifter, kostnadseffektivitet och till att förbygga obehörig tillgång till patientuppgifter.[236] Även skyddet av patienters integritet och personuppgifter ska behandlas i ledningssystemet för kvalitetsarbete och patientsäkerhet. Ledningssystemet ska tillgodose patientpersonuppgifternas tillgänglighet, riktighet, konfidentialitet, spårbarhet, och baseras på ISO/IEC 27000-serien.[237] En övergripande summering av regelverk och krav på detta område framställs i tabell 10:

[233] Se exempelvis summering i 2 kap. 2§ Socialstyrelsens föreskrifter och allmänna råd om ledningssystem för systematiskt kvalitetsarbete, SOSFS 2011:9 och HSLF-FS 2017:40.
[234] Patientdatalag (2008:355); Patientdataförordning (2008:360).
[235] Socialstyrelsens föreskrifter och allmänna råd om journalföring och behandling av personuppgifter i hälso- och sjukvården. HSLF-FS 2016:40.
[236] 1 kap. 2§ Patientdatalag (2008:355).
[237] 3 kap. 1§ Socialstyrelsens föreskrifter och allmänna råd om journalföring och behandling av personuppgifter i hälso- och sjukvården. HSLF-FS 2016:40.

Tabell 10. Skydd patientdata.

Styrning	Upprätta en informationssäkerhetspolicy med mål och inriktning för verksamhetens informationssäkerhet. Planera för funktionsstörning av informationssystem som behandlar personuppgifter.[238]
Bedömning	Löpande, dokumenterad riskanalys för att bedöma sannolikheten och konsekvenserna av oönskade händelser som kan medföra att patientdatakraven inte uppfylls. Dokumentera patientsäkerhetsberättelse, inklusive riskanalys och uppföljningar.[239]
Åtgärdande	Vidta tekniska och organisatoriska säkerhetsåtgärder avseende bland annat informationssystems drift, upphandling och utveckling, funktionsstörningar, säkerhetskopiering, fysiskt skydd av informationssystem, öppna nät, medium för informationslagring, sekretess, behörigheter och uppgiftsåtkomst.[240]
Incident-hantering	Sammanställ information om incidenter som har påverkat informationssäkerheten och kan orsaka vårdskada.[241]
Revision	Följ upp behörigheter och utvärdera skyddet mot olovlig åtkomst.[242]

9.1.4 Medicintekniska produkter

Regleringen av medicintekniska produkter riktar sig främst mot tillverkare av produkter som ska användas för att:

- Påvisa, förebygga, övervaka, behandla eller lindra en sjukdom.
- Påvisa, övervaka, behandla, lindra eller kompensera en skada eller en funktionsnedsättning.
- Undersöka, ändra eller ersätta anatomin eller en fysiologisk process.
- Kontrollera befruktning.[243]

För att släppas på marknaden och kunna tas i bruk ska de uppfylla de säkerhets- och prestandakrav som ställs i bilagorna till EU:s förordningar på området, såsom

[238] 3 kap. 4, 11 §§ Socialstyrelsens föreskrifter och allmänna råd om journalföring och behandling av personuppgifter i hälso- och sjukvården. HSLF-FS 2016:40.

[239] 3 kap. 5§, 7 kap. 1§ Socialstyrelsens föreskrifter och allmänna råd om journalföring och behandling av personuppgifter i hälso- och sjukvården. HSLF-FS 2016:40.

[240] 5 kap. 5§, 6 kap. 6§ Patientsäkerhetslag (2010:659).; 3 § Patientdataförordning (2008:360); Socialstyrelsens föreskrifter och allmänna råd om journalföring och behandling av personuppgifter i hälso- och sjukvården. HSLF-FS 2016:40.

[241] 3 kap. 6§ Socialstyrelsens föreskrifter och allmänna råd om journalföring och behandling av personuppgifter i hälso- och sjukvården. HSLF-FS 2016:40.

[242] 3 kap. 6, 18 §§, 4 kap. 3§ Socialstyrelsens föreskrifter och allmänna råd om journalföring och behandling av personuppgifter i hälso- och sjukvården. HSLF-FS 2016:40.

[243] 2 §, Lag (1993:584) om medicintekniska produkter; artikel 2 Europaparlamentets och rådets förordning (EU) 2017/745 av den 5 april 2017 om medicintekniska produkter, om ändring av direktiv 2001/83/EG, förordning (EG) nr 178/2002 och förordning (EG) nr 1223/2009 och om upphävande av rådets direktiv 90/385/EEG och 93/42/EEG (Text av betydelse för EES.) OJ L 117; Artikel 2 Europaparlamentets och rådets förordning (EU) 2017/746 av den 5 april 2017 om medicintekniska produkter för in vitro-diagnostik och om upphävande av direktiv 98/79/EG och kommissionens beslut 2010/227/EU (Text av betydelse för EES.). OJ L 117.

att inte äventyra kliniska tillstånd, säkerhet, eller hälsa, [244] uppfylla lämplighetskraven i lagen om medicintekniska produkter.[245] krav utifrån Läkemedelsverkets föreskrifter för tillverkare och Socialstyrelsen föreskrifter för medicintekniska produkter som tillverkas inom hälso- och sjukvården.[246]

Kraven på tillverkarna av medicintekniska produkter är mycket omfattande och kan inte alla redovisas här. Övergripande innebär de dock att tillverkare, bland annat, ska ha följande förutsättningar på plats enligt tabell 11 nedan: [247]

Tabell 11. Säkerhets- och prestandakrav medicintekniska produkter.

Riskhanterings-system	Dokumenterad, kontinuerlig, iterativ och systematisk riskhantering, inklusive riskhanteringsplan, riskbedömningar och faroanalys, vidta kontrollåtgärder och utvärderingar av risker och faror.
Riskkontroll-åtgärder	Vidta riskkontrollåtgärder som överensstämmer med säkerhetsprinciper och tar hänsyn till det tekniska utvecklingsstadiet för att, bland annat, eliminera och minimera risker, vidta skyddsåtgärder, inklusive varningssignaler, och tillhandahålla information om säkerhet och risker. Riskeliminering och riskminimering i produktdesignen ska främja patientsäkerhet och ta hänsyn till användarens kunskap. Kända risker ska minimeras till en acceptable nivå.
Säker prestanda	Produkten ska inte äventyra användarens eller någon annans hälsa eller säkerhet och ska ha anvisningar för underhåll. Prestandan ska inte påverkas negativt av transport och lagring.

De praktiska kraven på användarna av medicintekniska produkter fastställs främst i Socialstyrelsens föreskrifter om användning av medicintekniska produkter i hälso- och sjukvården.[248] Vårdgivaren ska möjliggöra säker användning och hantering av medicintekniska produkter genom sitt ledningssystem.[249] Standarden

[244] Bilaga I, 2 Europaparlamentets och rådets förordning (EU) 2017/745 av den 5 april 2017 om medicintekniska produkter, om ändring av direktiv 2001/83/EG, förordning (EG) nr 178/2002 och förordning (EG) nr 1223/2009 och om upphävande av rådets direktiv 90/385/EEG och 93/42/EEG (Text av betydelse för EES.) OJ L 117; Bilaga I, Europaparlamentets och rådets förordning (EU) 2017/746 av den 5 april 2017 om medicintekniska produkter för in vitro-diagnostik och om upphävande av direktiv 98/79/EG och kommissionens beslut 2010/227/EU (Text av betydelse för EES.). OJ L 117; 4-5§§.

[245] 5 §, Lag (1993:584) om medicintekniska produkter.

[246] 4 §, Förordning (1993:876) om medicintekniska produkter.

[247] Läkemedelsverket (2020). *Läkemedelsverkets föreskrifter - LVFS och HSLF-FS - Fritext: medicintekniska produkter* https://www.lakemedelsverket.se/sv/lagar-och-regler/foreskrifter?q=medicintekniska%20produkter%20&c2=0. (besökt 20-09-22); Bilaga I, 2 Europaparlamentets och rådets förordning (EU) 2017/745 av den 5 april 2017 om medicintekniska produkter, om ändring av direktiv 2001/83/EG, förordning (EG) nr 178/2002 och förordning (EG) nr 1223/2009 och om upphävande av rådets direktiv 90/385/EEG och 93/42/EEG (Text av betydelse för EES.) OJ L 117; Bilaga I, Europaparlamentets och rådets förordning (EU) 2017/746 av den 5 april 2017 om medicintekniska produkter för in vitro-diagnostik och om upphävande av direktiv 98/79/EG och kommissionens beslut 2010/227/EU (Text av betydelse för EES.). OJ L 117; Bilaga 1 Läkemedelsverkets föreskrifter om medicintekniska produkter. LVFS 2003:11.

[248] Socialstyrelsens föreskrifter om användning av medicintekniska produkter i hälso- och sjukvården, SOSFS 2008:1.

[249] 3 kap. 4 § Socialstyrelsens föreskrifter om användning av medicintekniska produkter i hälso- och sjukvården, SOSFS 2008:1.

ISO 13485:2003 Medicintekniska produkter – Ledningssystem för kvalitet – Krav för regulatoriska ändamål, nämns i detta sammanhang. I hänseende till informationssystem uppmanar föreskrifterna även vårdare att ”Se SS-ISO/IEC 27001: 2006 Ledningssystem för informationssäkerhet – Krav samt SS-ISO/IEC 27002:2005 Riktlinjer för styrning av informationssäkerhet”.[250] Vårdgivare ska tillsätta en verksamhetschef som tillgodoser att endast säkra medicintekniska produkter och anslutna informationssystem, används, föreskrivs, utlämnas till, och tillförs patienter, samt anmäler negativa händelser och tillbud.[251] Personalen som hanterar produkterna ska även ha kunskap om åtgärder för att begränsa vårdskador och negativa händelser. Personalens ansvar omfattar också säkerhetsåtgärder för produkters anpassning till patienters hemmiljö samt att informera patienten om tillverkarens säkerhetsföreskrifter.[252]

Personalen ska även utföra tillverkarens kontroll av produkterna innan de används på patienter.[253] Vid negativa händelser och tillbud med medicintekniska produkter ska vårdgivaren bland annat:

- Utreda och bedöma händelsen.
- Anmäla händelsen vid dödsfall och försämring av hälsotillstånd.
- Omhänderta produkten.
- Följa upp utredningarna av händelsen och informera personalen om resultatet.[254]

9.2 Övriga regler och bestämmelser

9.2.1 E-hälsa

Inom EU regleras gränsöverskridande sjukvård genom direktiv 2011/24/EU.[255] Direktivets bestämmelser syftar bland annat till att säkerställa ”säker och högkvalitativ gränsöverskridande hälso- och sjukvård, […] mellan medlemsstater”.[256] Direktivet upprättar även ett frivilligt nätverk för att koppla ihop nationella

[250] 2 kap. 1 § Socialstyrelsens föreskrifter om användning av medicintekniska produkter i hälso- och sjukvården, SOSFS 2008:1.
[251] 3 kap. 6-7 §§ Socialstyrelsens föreskrifter om användning av medicintekniska produkter i hälso- och sjukvården. SOSFS 2008:1.
[252] 3 kap. 9 § Socialstyrelsens föreskrifter om användning av medicintekniska produkter i hälso- och sjukvården. SOSFS 2008:1.
[253] 3 kap. 9 § Socialstyrelsens föreskrifter om användning av medicintekniska produkter i hälso- och sjukvården. SOSFS 2008:1.
[254] 6 kap. Socialstyrelsens föreskrifter om användning av medicintekniska produkter i hälso- och sjukvården. SOSFS 2008:1.
[255] Europaparlamentets och rådets direktiv 2011/24/EU av den 9 mars 2011 om tillämpningen av patienträttigheter vid gränsöverskridande hälso- och sjukvård. EUT L 88, 4.4.2011.
[256] Artikel 1, direktiv 2011/24/EU.

myndigheter i EU som är ansvariga för digitala hälso- och sjukvårdstjänster, så kallad e-hälsa.[257] Nätverkets ansvarsområden omfattar bland annat:

- Arbete mot driftskompatibilitet, tillförlitlighet, säkerhet och kontinuitet.
- Riktlinjer om hantering av uppgifter och medicinsk information.
- Gemensamma åtgärder för identifiering och autentisering.

Kommissionen har dessutom antagit ett genomförandebeslut med regler om förvaltning och drift av e-hälsa.[258] Avseende säkerhet formaliserar genomförandebeslutet främst de bestämmelser som redan fastställts genom direktiv 2011/24/EU. Kommissionens handlingsplan för e-hälsa upplyser även om fortlöpande arbete med säkerhet och integritet under åren 2012 till 2020.[259]

9.2.2 Fastighetsautomation

Ökad digitalisering har genom lokala och överordnade styr- och övervakningssystem lett till en högre grad av fastighetsautomation i sjukhusbyggnader. Fastighetsautomation innebär att system för exempelvis värme, kyla och ventilation styrs automatiskt, vilket medför effektivare energianvändning och möjlighet att snabbt hantera driftsstörningar. Detta innebär att eventuella problem med styr- och övervakningssystemen, oavsett orsakerna bakom dessa, kan resultera i stor påverkan på ett sjukhus möjlighet att bedriva verksamheten.[260]

I dagsläget saknas nationell styrning för säkerhetsarbete med informations- och styrsystem inom fastighetsautomation i hälso- och sjukvården. Ett antal regioner är mer aktiva än andra med säkerhetsarbetet, men frågan skulle behöva regleras centralt. Fokus för nuvarande säkerhetsarbete tycks främst ligga på frågor såsom underhåll av systemen, medan behov finns att även fokusera på till exempel intrång i systemen. Systemen behöver exempelvis designas med separata nätverk och fungera autonomt, utan koppling till internet, för att vara säkra mot intrång. Det aktiva it-säkerhetsarbete som i dagsläget är standard inom administrativ it saknas många gånger i fastighetsautomationsnätverk. Det kan gälla sådant som malwareskydd (antivirusprogram), korrekt konfigurerade brandväggar, inaktiverade tjänster som inte används eller regelbunden patchning/uppdatering. Även spårbarheten är i många fall bristfällig. Inom administrativ it loggas normalt alla händelser och förändringar, vilket sällan i samma grad görs inom fastighetsautomation.[261]

---

[257] Artikel 14, direktiv 2011/24/EU.

[258] 2011/890/EU: Kommissionens genomförandebeslut av den 22 december 2011 om regler för inrättande, förvaltning och drift av ett nätverk av nationella myndigheter med ansvar för e-hälsa EUT L 344, 28.12.2011.

[259] Meddelande från Kommissionen till Europaparlamentet, Rådet, Europeiska ekonomiska och sociala kommittén samt Regionkommittén. Handlingsplanen för e-hälsa 2012–2020 - Innovativ Hälsovård för det 21:a århundradet. /* COM/2012/0736 final */.

[260] Myndigheten för samhällsskydd och beredskap, Den robusta sjukhusbyggnaden - 2020 En vägledning för funktionssäkra sjukhusfastigheter, Remissutgåva, s.28f, tillgänglig på https://sfvh.se/a/den-robusta-sjukhusbyggnaden-remiss-fran-msb (besökt 21-01-20).

[261] Personlig kommunikation med Anders Gidrup, säkerhetschef Locum, 21-01-21.

10 Reglering inom andra områden

Utöver den sektorsövergripande reglering som uttryckligen tar sikte på säkerhet i teknik (kapitel 2), bör det även nämnas att det finns annan reglering som medför krav på cybersäkerhet. I tabellen 12 nedan lyfts några exempel på krav angående konfidentialitet, riktighet och tillgänglighet från olika lagrum. Varken exemplen eller lagarna de är hämtade ifrån är menade att utgöra en komplett lista av annan reglering. Exemplen visar att regleringen av informationssystem innehåller omfattande och spridda krav på hur olika typer av information ska hanteras.

Tabell 12. Reglering andra områden.

Lagrum	Konfidentialitet	Riktighet	Tillgänglighet
Offentlighet och sekretess[262]	Förbud mot utnyttjandet av sekretessreglerad uppgift.	Allmän handling ska skiljas från annan handling. Ändring, tillförande av uppgift och gallring bör vara spårbart.	Utlämnande av allmän handling.
Arkivlagen[263]	Skydda arkivet mot obehörig åtkomst.	Skydda arkivet mot förstörelse, skada och tillgrepp.	Rätten att ta del av allmänna handlingar underlättas.
Lag om offentlig upphandling[264]	Uppgifter från leverantör ska bevaras säkert. Öppnande av anbud ska endast ske vid tidsfrist.	Rättelse, förtydligande och komplettering i anbud.	Upphandlingar ska genomföras på ett öppet sätt.

Regeringen beslutade under 2019[265] att ge i uppdrag åt en särskild utredare att kartlägga och analysera statliga myndigheters behov av säker och kostnadseffektiv it-drift samt hur dessa behov kan tillgodoses. Utredaren fick även i uppdrag att analysera säkerhetsmässiga och rättsliga förutsättningar för samordnad statlig it-drift och lämna förslag på mer varaktiga former för sådan it-drift (om det bedöms lämpligt ur ett säkerhetsperspektiv), samt ge nödvändiga författningsförslag. Ett delbetänkande har publicerats[266] med bland annat ett förslag till lag om ändring i offentlighets- och sekretesslagen. Ett slutbetänkande ska redovisas senast den 15

[262] Tryckfrihetsförordning (1949:105); offentlighets- och sekretesslag (2009:400); Offentlighets- och sekretessförordning (2009:641).
[263] Arkivlag (1990:782); arkivförordning (1991:446).
[264] Lag (2016:1145) om offentlig upphandling; upphandlingsförordning (2016:1162).
[265] Kommittédirektiv 2019:64, Säker och kostnadseffektiv it-drift för den offentliga förvaltningen.
[266] SOU 2021:1, Säker och kostnadseffektiv it-drift – rättsliga förutsättningar för utkontraktering.

oktober 2021. Det bör vara av intresse att följa vad utredningens betänkanden och eventuella författningsförändringar kommer att innebära.

Enligt brottsbalkens bestämmelser om dataintrång[267] är det förbjudet att olovligen bereda sig tillgång till en uppgift som är avsedd för automatiserad behandling eller olovligen ändra, utplåna, blockera eller i register föra in en sådan uppgift. Det är även förbjudet att olovligen, genom någon annan liknande åtgärd, allvarligt störa eller hindra användningen av en sådan uppgift.

Lag om företagshemligheter,[268] reglerar skadestånd, vitesförbud och straff vid obehöriga angrepp på företagshemligheter. Lagen genomför delvis Europaparlamentets och rådets direktiv 2016/943/EU om skydd mot att icke röjd know-how och företagsinformation olagligen anskaffas, utnyttjas och röjs.[269] Med företagshemlighet avses information om affärs- eller driftförhållanden i en näringsidkares rörelse, som inte är allmänt känd hos eller lättillgänglig för den som normalt har tillgång till information av det aktuella slaget och som innehavaren har vidtagit rimliga åtgärder för att hemlighålla. Att röja sådan information, med syftet att medföra skada i konkurrenshänseende för innehavaren, är olagligt.[270]

Flera av de sektorer som ingår i denna rapport regleras också av lagen om upphandling inom försörjningssektorerna.[271] Även här kan finnas relevanta regleringar kring hur kravställning ska göras i offentliga upphandlingar som behöver analyseras.

[267] 4 kap. 9c och 10 §§ Brottsbalk (1962:700).
[268] Lag (2018:558) om företagshemligheter.
[269] Europaparlamentets och rådets direktiv 2016/943/EU av den 8 juni 2016 om skydd mot att icke röjd know-how och företagsinformation (företagshemligheter) olagligen anskaffas, utnyttjas och röjs.
[270] 1-2 §§ Lag (2018:558) om företagshemligheter.
[271] Lag (2016:1146) om upphandling inom försörjningssektorerna.

11 Ordlista juridiska termer

Begrepp	**Förklaring**[272]
EU-direktiv	EU-direktiv innehåller bindande bestämmelser som riktar sig till EU:s medlemsländer. Det är bara direktivets resultat och när det ska vara uppnått som är bindande. Medlemsländerna beslutar själva vad de ska göra för att uppnå resultatet.
EU-förordning	En EU-förordning gäller alla EU:s medlemsländer, de företag och myndigheter som är verksamma i länderna samt ländernas medborgare. De har samma verkan som lagar och gäller i medlemsländerna precis som de är skrivna. Det betyder att de inte får omarbetas eller justeras med hänsyn till medlemsländernas egna förhållanden.
Föreskrift	Riksdag och regering har gett (bemyndigat) vissa statliga myndigheter rätt att besluta om föreskrifter inom sitt verksamhetsområde. Myndighetsföreskrifterna publiceras i den författningssamling som hör till myndigheten.
Författning	Författning är en samlande beteckning för lagar, förordningar och myndighetsföreskrifter.
Förordning	Förordningar är regler som regeringen beslutar utan riksdagens medverkan. De kan till exempel reglera de statliga myndigheternas arbete. Alla förordningar publiceras i Svensk författningssamling (SFS).
Instruktion	En instruktion är en förordning, utfärdad av regeringen, som reglerar en statlig myndighets arbete.
Kommittédirektiv	När regeringen utser en kommitté får den i uppdrag att utreda en viss fråga. Regeringen anger riktlinjerna för arbetet i ett kommittédirektiv. Direktivet talar bland annat om vilken fråga som ska utredas, vilka problem som är viktiga att ta hänsyn till och när utredningen ska vara färdig.
Lag	Lagar antas av riksdagen och en lag kan den bara ändras eller upphävas genom att riksdagen beslutar om en ny lag. Alla lagar publiceras i Svensk författningssamling (SFS).
Myndighets Författningssamling	Vissa statliga myndigheter har sina egna författningssamlingar där deras myndighetsföreskrifter publiceras.
Proposition	En proposition är ett förslag från regeringen till riksdagen. En proposition kan innehålla förslag till nya lagar, ändringar av lagar eller nya riktlinjer.
Regleringsbrev	Regeringen styr statliga myndigheter genom årliga regleringsbrev. Ett regleringsbrev talar om vilka mål en myndighet ska uppnå med sin verksamhet och hur mycket pengar den får till sitt förfogande.
Statens offentliga utredningar, SOU	Slutsatser och förslag från en särskild utredare eller från en kommitté som regeringen har tillsatt redovisas som regel i ett betänkande. Betänkandet publiceras i serien Statens offentliga utredningar (SOU).
Svensk Författningssamling, SFS	Svensk författningssamling (SFS) är en serie där lagar som riksdagen har beslutat och förordningar som regeringen har beslutat kungörs.

[272] Begreppsförklaringarna kommer från https://www.lagrummet.se/lar-dig-mer/ordlistan-a-o#F (Besökt 21-01-13).

12 Referenser

12.1 Inledning

Lagar

SFS 2018:585 Säkerhetsskyddslag

EU direktiv och förordningar

Europaparlamentets och Rådets Direktiv (EU) 2016/1148 av den 6 juli 2016 om åtgärder för en hög gemensam nivå på säkerhet i nätverks- och informationssystem i hela unionen.

Förslag till Europaparlamentets och Rådets Förordning om Enisa, ”EU:s cybersäkerhetsbyrå”, och om upphävande av förordning (EU) nr 526/2013, och om cybersäkerhetscertifiering av informations- och kommunikationsteknik (”cybersäkerhetsakten”). COM/2017/0477 final/2 - 2017/0225 (COD).

Utredningar

Lindgren, F. (2013). Regelverk och krav inom området säkerhet i industriella informations- och styrsystem. FOI Memo 4415.

Mossberg Sonnek, K och Lindgren, F. (2015). NCS3 – Regelverk och krav inom området industriella informations- och styrsystem. FOI-R--4197--SE.

Webbsidor

https://ec.europa.eu/digital-single-market/en/news/proposal-directive-measures-high-common-level-cybersecurity-across-union

https://www.msb.se/sv/amnesomraden/informationssakerhet-cybersakerhet-och-sakra-kommunikationer/sakerhet-i-cyberfysiska-system/industriella-information--och-styrsystem/

12.2 Sektorsövergripande reglering

Lagar

SFS 1985:125 Tandvårdslag

SFS 1992:1403 Lag om totalförsvar och höjd beredskap i fråga om civil verksamhet

SFS 1997:857 Ellag

SFS 2006:412	Lag om allmänna vattentjänster
SFS 2009:366	Lag om handel med läkemedel
SFS 2009:400	Offentlighets- och sekretesslag
SFS 2010:305	Skyddslag
SFS 2011:710	Lag om certifiering av transmissionsnätsföretag för el
SFS 2017:30	Hälso- och sjukvårdslag
SFS 2018:218	Lag med kompletterande bestämmelser till EU:s dataskyddsförordning
SFS 2018:585	Säkerhetsskyddslag
SFS 2018:1174	Lag om informationssäkerhet för samhällsviktiga och digitala tjänster

Förordningar

SFS 2009:641	Offentlighets- och sekretessförordning
SFS 2011:931	Förordning om planering för prioritering av samhällsviktiga elanvändare
SFS 2015:1052	Förordning om krisberedskap och bevakningsansvariga myndigheters åtgärder vid höjd beredskap
SFS 2018:658	Säkerhetsskyddsförordning
SFS 2018:1175	Förordning om informationssäkerhet för samhällsviktiga och digitala tjänster

Föreskrifter

Energimarknadsinspektionen

EIFS 2012:4	Energimarknadsinspektionens föreskrifter och allmänna råd om redovisning av nätverksamhet

Myndigheten för samhällsskydd och beredskap

MSBFS 2018:7	Myndigheten för samhällsskydd och beredskaps föreskrifter om anmälan och identifiering av leverantörer av samhällsviktiga tjänster
MSBFS 2018:8	Myndigheten för samhällsskydd och beredskaps föreskrifter om informationssäkerhet för leverantörer av samhällsviktiga tjänster

MSBFS 2018:9	Myndigheten för samhällsskydd och beredskaps föreskrifter om rapportering av incidenter för leverantörer av samhällsviktiga tjänster
MSBFS 2018:11	Myndigheten för samhällsskydd och beredskaps föreskrifter om frivillig rapportering av incidenter i tjänster som är viktiga för samhällets funktionalitet.
MSBFS 2020:6	Myndigheten för samhällsskydd och beredskaps föreskrifter om informationssäkerhet för statliga myndigheter
MSBFS 2020:7	Myndigheten för samhällsskydd och beredskaps föreskrifter om säkerhetsåtgärder i informationssystem för statliga myndigheter
MSBFS 2020:8	Myndigheten för samhällsskydd och beredskaps föreskrifter om rapportering av it-incidenter för statliga myndigheter

Säkerhetspolisen

PMFS 2019:2	Säkerhetspolisens föreskrifter om säkerhetsskydd

EU direktiv och förordningar

Rådets direktiv 98/83/EG av den 3 november 1998 om kvaliteten på dricksvatten. OJ L 330

Europaparlamentets och rådets direktiv 2009/72/EG av den 13 juli 2009 om gemensamma regler för den inre marknaden för el och om upphävande av direktiv 2003/54/EG (Text av betydelse för EES). OJ L 211

Europaparlamentets och rådets direktiv 2011/24/EU av den 9 mars 2011 om tillämpningen av patienträttigheter vid gränsöverskridande hälso- och sjukvård. OJ L 88

Europaparlamentets och rådets direktiv 2012/34/EU av den 21 november 2012 om inrättande av ett gemensamt europeiskt järnvägsområde Text av betydelse för. EES OJ L 343

Europaparlamentets och rådets direktiv (EU) 2016/1148 av den 6 juli 2016 om åtgärder för en hög gemensam nivå på säkerhet i nätverks- och informationssystem i hela unionen. OJ L 194.

Europaparlamentets och rådets förordning (EU) 2016/679 av den 27 april 2016 om skydd för fysiska personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter och om upphävande av direktiv 95/46/EG (allmän dataskyddsförordning) (Text av betydelse för EES) EUT L 119, 4.5.2016.

Europaparlamentets och rådets förordning (EU) 2019/881 av den 17 april 2019 om Enisa (Europeiska unionens cybersäkerhetsbyrå) och om cybersäkerhetscertifiering av informations- och kommunikationsteknik och om upphävande av förordning (EU) nr 526/2013 (cybersäkerhetsakten) (Text av betydelse för EES) PE/86/2018/REV/1. EUT L 151

Europeiska unionens stadga om de grundläggande rättigheterna. EUT C 326

Förordning (EU) 2019/881; Förslag till Europaparlamentets och Rådets förordning om Enisa, ”EU:s cybersäkerhetsbyrå”, och om upphävande av förordning (EU) nr 526/2013, och om cybersäkerhetscertifiering av informations- och kommunikationsteknik (”cybersäkerhetsakten”). COM(2017) 477 final

Meddelande från Kommissionen till Europaparlamentet, Rådet, Europeiska Ekonomiska och Sociala Kommittén samt regionkommittén. Prioriteringar för informations- och kommunikationsteknisk standardisering på den digitala inre marknaden. COM/2016/0176 final

Utredningar

En ny säkerhetsskyddslag. SOU 2015:25

Kommittédirektiv Cybersäkerhet – genomförandet av cybersäkerhetsakten och vissa åtgärder till skydd för säkerhetskänslig verksamhet. Dir. 2019:73.

Rapporter, artiklar och dokument

Datainspektionen. (2008). Säkerhet för personuppgifter. Datainspektionens allmänna råd

Data Protection Working Party. (2017). Opinion 2/2017 on data processing at work. 17/EN WP 249

Guide to Industrial Control Systems (ICS) Security. NIST Special Publication 800-82 (Revision 2)

Kobara, K. (2016). Cyber physical Security for Industrial Control Systems and IOT. IECE Transactions on Information and Systems 99(4)

Mossberg Sonnek, K och Lindgren, F. (2015). NCS3 – Regelverk och krav inom området industriella informations- och styrsystem. FOI-R--4197--SE

Radic, J. P., Frank, J. (2018). Projekt för styrsystem för belysning och styrning på distans av bangårdsbelysning. Trafikverket 2018:176; Trafikverket. (2018)

Sagehi, A. R., Wachsmann, C., Waidner, M. (2015). Security and Privacy Challenges in Industrial Internet of Things. IEEE 2015/2015 52nd ACM/EDAC

Säkerhetspolisen. (2019). Vägledning i säkerhetsskydd: Fysisk säkerhet

Säkerhetspolisen. (2019). Vägledning i säkerhetsskydd: Informationssäkerhet

Säkerhetspolisen. (2019). Vägledning i säkerhetsskydd: Introduktion till säkerhetsskydd

Säkerhetspolisen. (2019). Vägledning i säkerhetsskydd: Personalsäkerhet

Säkerhetspolisen. (2019). Vägledning i säkerhetsskydd: Säkerhetsskyddsanalys

Säkerhetspolisen (2019). Vägledning i säkerhetsskydd: Säkerhetsskyddad upphandling

Webbsidor

Johan Eriksson. (2017). Hur klokt är det att fjärrstyra flygtrafiken? https://kuriren.nu/nm4701463

Jonas Olsson. (2019). Svenska Kraftnät medger säkerhetsbrister. https://www.svt.se/nyheter/inrikes/svenska-kraftnat-medger-sakerhetsbrister

Nytt styrsystem på Kvicksundsbron. https://www.trafikverket.se/om-oss/nyheter/Lansvisa-nyheter/Vastmanland/2018/nytt-styrsystem-pa-kvicksundsbron/

Oskar Alex. (2019). Snart kan robotar sköta flygplatserna. https://fof.se/artikel/snart-kan-robotar-skota-flygplatserna

Svenska kraftnät. (2019). Kommentar till medias uppgifter om tillgång till styrsystem. https://www.svk.se/press-och-nyheter/nyheter/allmanna-nyheter/2019/kommentar-till-medias-uppgifter-om-tillgang-till-styrsystem/

Rättsfall

Eur. Court HR, Barbulescu v. Romania, judgement of 5 September 2017, application no. 61496/08

Eur. Court HR, Copland v. United Kingdom, judgement of 3 April 2007, application no. 62617/00

Eur. Court HR, Halford v. The United Kingdom, judgement of 25 June 1997, Reports of Judgements and Decisions 1997-III

Eur. Court HR, Niemietz v. Germany judgement of 16 December 1992, Series A no.251-B

12.3 Elproduktion och eldistribution

Lagar

SFS 1984:3 Lag om kärnteknisk verksamhet

SFS 1997:288 Elberedskapslag

SFS 1997:857 Ellag

SFS 2003:778 Lag om skydd mot olyckor

SFS 2018:396 Strålskyddslag

SFS 2018:585 Säkerhetsskyddslag

Förordningar

SFS 1984:14 Förordning om kärnteknisk verksamhet

SFS 1994:1806 Förordning om systemansvaret för el

SFS 1997:294 Förordning om elberedskap

SFS 2013:208 Elförordning

SFS 2014:214 Förordning om dammsäkerhet

SFS 2018:506 Strålskyddsförordning

SFS 2018:658 Säkerhetsskyddsförordning

Föreskrifter

Affärsverket svenska kraftnät

SvKFS 2005:2 Affärsverket svenska kraftnäts föreskrifter och allmänna råd om driftsäkerhetsteknisk utformning av produktionsanläggningar

SvKFS 2013:2 Affärsverket svenska kraftnäts föreskrifter och allmänna råd om elberedskap

SvKFS 2019:1 Affärsverket svenska kraftnäts föreskrifter och allmänna råd om säkerhetsskydd

Energimarknadsinspektionen

EIFS 2013:3 Energimarknadsinspektionens föreskrifter och allmänna råd om risk- och sårbarhetsanalyser och åtgärdsplaner avseende leveranssäkerhet i elnäten

Strålsäkerhetsmyndigheten

SSMFS 2008:1 Strålsäkerhetsmyndighetens föreskrifter och allmänna råd om säkerhet i kärntekniska anläggningar (konsoliderad version - ändringar införda genom SSMFS 2010:3, 2011:3, 2014:3, 2017:1, 2018:12)

SSMFS 2008:12 Strålsäkerhetsmyndighetens föreskrifter och allmänna råd om fysiskt skydd av kärntekniska anläggningar (konsoliderad version - ändringar införda t.o.m. SSMFS 2018:14)

SSMFS 2008:17 Strålsäkerhetsmyndighetens föreskrifter och allmänna råd om konstruktion och utförande av kärnkraftsreaktorer

SSMFS 2014:2 Strålsäkerhetsmyndighetens föreskrifter om beredskap vid kärntekniska anläggningar (konsoliderad version - ändringar införda t.o.m. SSMFS 2018:26)

EU direktiv och förordningar

Rådets direktiv 2013/59/ Euratom av den 5 december 2013 om fastställande av grundläggande säkerhetsnormer för skydd mot de faror som uppstår till följd av exponering för joniserande strålning, och om upphävande av direktiven 89/618/Euratom, 90/641/Euratom, 96/29/Euratom, 97/43/Euratom och 2003/122/Euratom

Rådets direktiv 2013/59/ Euratom av den 5 december 2013 om fastställande av grundläggande säkerhetsnormer för skydd mot de faror som uppstår till följd av exponering för joniserande strålning, och om upphävande av direktiven 89/618/Euratom, 90/641/Euratom, 96/29/Euratom, 97/43/Euratom och 2003/122/Euratom

Rapporter, artiklar och dokument

Vägledning - skyddsobjekt inom energiförsörjningen, 2012-06-11, Dnr: 2011/1140

Webbsidor

https://www.stralsakerhetsmyndigheten.se/regler/foreskrifter/oversyn-av-vara-foreskrifter/

12.4 Dricksvattenproduktion och vattendistribution

Lagar

SFS 1977:1160 Arbetsmiljölag

SFS 1998:808 Miljöbalk

SFS 2006:412 Lag om allmänna vattentjänster

SFS 2006:804 Livsmedelslag

Förordningar

SFS 1977:1166 Arbetsmiljöförordning

SFS 1998:899 Förordning om miljöfarlig verksamhet och hälsoskydd

SFS 2006:813	Livsmedelsförordning
SFS 2007:701	Förordning om allmänna vattentjänster

Föreskrifter

Livsmedelsverket

LIVSFS 2008:13	Åtgärder mot sabotage och annan skadegörelse riktad mot dricksvattenanläggningar (konsoliderad version - innehåller ändringarna LIVSFS 2013:5)

Tillkännagivanden

SFS 2019:716	Tillkännagivande av de EU-bestämmelser som livsmedelslagen (2006:804) kompletterar

Rapporter, artiklar och dokument

Svenskt Vatten, Råd och riktlinjer – Fysiskt och tekniskt skydd för dricksvatten, december 2011

Svenskt Vatten, Sammanställning av råd och riktlinjer för ansvariga inom dricksvattenproduktion, Rapport R1, April 2017

Svenskt vatten, Säkerhetshandbok för dricksvattenproducenter, Publikation U12, 2012

Webbsidor

http://kontrollwiki.livsmedelsverket.se/artikel/361/atgarder-mot-sabotage-och-annan-skadegorelse

https://www.livsmedelsverket.se/produktion-handel--kontroll/nkp-webben

12.5 Fjärrvärme/-kyla – produktion och distribution

Lagar

SFS 1962:700	Brottsbalk
SFS 1970:994	Jordabalk
SFS 1977:1160	Arbetsmiljölag
SFS 1998:808	Miljöbalk
SFS 2008:263	Fjärrvärmelag

Förordningar

SFS 2008:526 Fjärrvärmeförordning

SFS 2016:742 Förordning med instruktion för Energimarknadsinspektionen

Föreskrifter

Arbetsmiljöverket

AFS 2017:3 Arbetsmiljöverkets föreskrifter om användning och kontroll av trycksatta anordningar (Ändringar införda t.o.m. den 29 mars 2019, AFS 2019:1)

Rapporter, artiklar och dokument

Svensk Fjärrvärme, Säkerhet i fjärrvärmeanläggningar – Regler och råd för riskbedömning, 2004:2.

Webbsidor

https://www.energiforetagen.se/medlemsportalen/listsida/fjarrvarmefragor/fjarrvarmedistribution/tekniska-bestammelser/

12.6 Kemisk processindustri

Lagar

SFS 1998:808 Miljöbalk

SFS 1999:381 Lag om åtgärder för att förebygga och begränsa följderna av allvarliga kemikalieolyckor och

SFS 2003:778 Lag om skydd mot olyckor

SFS 2010:900 Plan- och bygglag

SFS 2010:1011 Lag om brandfarliga och explosiva varor

Förordningar

SFS 1998:899 Förordning om miljöfarlig verksamhet och hälsoskydd

SFS 1998:901 Förordning om verksamhetsutövares egenkontroll

SFS 2003:789 Förordning om skydd mot olyckor

SFS 2010:1075 Förordning om brandfarliga och explosiva varor

SFS 2011:13 Miljötillsynsförordning

SFS 2015:236 Förordning om åtgärder för att förebygga och begränsa följderna av allvarliga kemikalieolyckor

Föreskrifter

Myndigheten för samhällsskydd och beredskap

MSBFS 2015:8	Myndigheten för samhällsskydd och beredskaps föreskrifter om åtgärder för att förebygga och begränsa följderna av allvarliga kemikalieolyckor

EU direktiv och förordningar

2012/18/EU	Europaparlamentets och rådets direktiv av den 4 juli 2012 om åtgärder för att förebygga och begränsa faran för allvarliga olyckshändelser där farliga ämnen ingår och om ändring och senare upphävande av rådets direktiv 96/82/EG
1272/2008 EG	Europaparlamentets och rådets förordning av den 16 december 2008 om klassificering, märkning och förpackning av ämnen och blandningar, ändring och upphävande av direktiven 67/548/EEG och 1999/45/EG samt ändring av förordning (EG) nr 1907/2006

12.7 Spårbunden trafik

Lagar

SFS 1990:1157	Lag om säkerhet vid tunnelbana och spårväg
SFS 2004:519	Järnvägslag
SFS 2010:305	Skyddslag

Förordningar

SFS 1990:1165	Förordning om säkerhet vid tunnelbana och spårväg.
SFS 2004:526	Järnvägsförordning

Föreskrifter

Transportstyrelsen

TSFS 2013:44	Transportstyrelsens föreskrifter om säkerhetsstyrning och säkerhetsordning med säkerhetsbestämmelser inom tunnelbana och spårväg
TSFS 2015:34	Transportstyrelsens föreskrifter om säkerhetsstyrningssystem och övriga säkerhetsbestämmelser för infrastrukturförvaltare med säkerhetstillstånd samt järnvägsföretag med säkerhetsintyg

TSFS 2015:77 Transportstyrelsens föreskrifter om bedrivande av tågtrafik

EU direktiv och förordningar

Europarådets och parlamentets direktiv 2004/49/EG

Europaparlamentets och rådets direktiv 2008/57/EG

Kommissionens beslut 2012/757/EU av den 14 november 2012 om teknisk specifikation för driftskompatibilitet avseende delsystemet ”Drift och trafikledning” i järnvägssystemet i Europeiska unionen och om ändring av beslut 2007/756/EG, i lydelse enligt kommissionens beslut 2013/710/EU

Kommissionens genomförandeförordning (EU) nr 402/2013 av den 30 april 2013 om den gemensamma säkerhetsmetoden för riskvärdering och riskbedömning och om upphävande av förordning (EG) nr 352/2009.

12.8 Elektroniska kommunikationer

Lagar

SFS 2003:389 Lag om elektronisk kommunikation

SFS 2016:392 Radioutrustningslag

Förordningar

SFS 2003:396 Förordning om elektronisk kommunikation

SFS 2016:394 Radioutrustningsförordning

Föreskrifter

Post- och telestyrelsen

PTSFS 2007:2 Post- och telestyrelsens allmänna råd om god funktion och teknisk säkerhet samt uthållighet och tillgänglighet vid extraordinära händelser i fredstid

PTSFS 2014:1 Post- och telestyrelsens föreskrifter och allmänna råd om skyddsåtgärder för behandlade uppgifter

PTSFS 2015:2 Post- och telestyrelsens föreskrifter om krav på driftsäkerhet

PTSFS 2016:5 Post- och telestyrelsen föreskrifter om krav m.m. på radioutrustning

PTSFS 2020:1 Föreskrifter om ändring i Post- och telestyrelsens föreskrifter (PTSFS 2015:2) om krav på driftsäkerhet

EU direktiv och förordningar

Europaparlamentets och rådets direktiv 2002/21/EG av den 7 mars 2002 om ett gemensamt regelverk för elektroniska kommunikationsnät och kommunikationstjänster (ramdirektiv). EGT L 108, 24.4.2002

Europaparlamentets och rådets direktiv 2002/58/EG av den 12 juli 2002 om behandling av personuppgifter och integritetsskydd inom sektorn för elektronisk kommunikation (direktiv om integritet och elektronisk kommunikation. EGT L 201, 31.7.2002

Europaparlamentets och rådets direktiv 2014/53/EU av den 16 april 2014 om harmonisering av medlemsstaternas lagstiftning om tillhandahållande på marknaden av radioutrustning och om upphävande av direktiv 1999/5/EG Text av betydelse för EES, OJ L 153, 22.5.2014

Europaparlamentets och rådets direktiv (EU) 2016/1148 av den 6 juli 2016 om åtgärder för en hög gemensam nivå på säkerhet i nätverks- och informationssystem i hela unionen

Kommissionens genomförandeförordning (EU) 2018/151 av den 30 januari 2018 om tillämpningsföreskrifter för Europaparlamentets och rådets direktiv (EU) 2016/1148 om åtgärder för en hög gemensam nivå på säkerhet i nätverks- och informationssystem i hela unionen vad gäller närmare specificering av de aspekter som ska beaktas av leverantörer av digitala tjänster när de hanterar risker som hotar säkerheten i deras nät- och informationssystem samt parametrarna för fastställande av om en incident har avsevärd inverkan. C/2018/0471. EUT L 26, 31.1.2018

Rapporter, artiklar och dokument

Jonatan Westman, Erik Zouave, Christian Valassi. (2017). Cybersäkerhet på rymdarenan: Avskannande projekt 2017. FOI-D--0820--SE

Convention for the establishment of a European Space Agency (CSE/CS(73)19, rev.7)

Regulations of the European Space Agency: Security Regulations ESA/REG/004, rev.1

Regulations of the European Space Agency: Rules on information, Data and Intellectual Property Rights ESA/REG/008

12.9 Hälso- och sjukvård

Lagar

SFS 1993:584 Lag om medicintekniska produkter

SFS 2008:355	Patientdatalag
SFS 2010:659	Patientsäkerhetslag
SFS 2017:30	Hälso- och sjukvårdslag

Förordningar

SFS 1993:876	Förordning om medicintekniska produkter
SFS 2008:360	Patientdataförordning
SFS 2010:1369	Patientsäkerhetsförordning
SFS 2017:80	Hälso- och sjukvårdsförordning

Föreskrifter

Läkemedelsverket

Läkemedelsverkets föreskrifter om medicintekniska produkter. LVFS 2003:11

Socialstyrelsen

Socialstyrelsens föreskrifter om användning av medicintekniska produkter i hälso- och sjukvården, SOSFS 2008:1

Socialstyrelsens föreskrifter och allmänna råd om journalföring och behandling av personuppgifter i hälso- och sjukvården. HSLF-FS 2016:40

Socialstyrelsens föreskrifter och allmänna råd om ledningssystem för systematiskt kvalitetsarbete, SOSFS 2011:9 och HSLF-FS 2017:40

EU direktiv och förordningar

Europaparlamentets och rådets direktiv 2011/24/EU av den 9 mars 2011 om tillämpningen av patienträttigheter vid gränsöverskridande hälso- och sjukvård. EUT L 88, 4.4.2011

Europaparlamentets och rådets förordning (EU) 2017/745 av den 5 april 2017 om medicintekniska produkter, om ändring av direktiv 2001/83/EG, förordning (EG) nr 178/2002 och förordning (EG) nr 1223/2009 och om upphävande av rådets direktiv 90/385/EEG och 93/42/EEG (Text av betydelse för EES.). EUT L 117S

Europaparlamentets och rådets förordning (EU) 2017/746 av den 5 april 2017 om medicintekniska produkter för in vitro-diagnostik och om upphävande av direktiv 98/79/EG och kommissionens beslut 2010/227/EU (Text av betydelse för EES.). EUT L 117, 5.5.2017

Kommissionens genomförandebeslut 2011/890/EU av den 22 december 2011 om regler för inrättande, förvaltning och drift av ett nätverk av nationella myndigheter med ansvar för e-hälsa EUT L 344, 28.12.2011

Meddelande från Kommissionen till Europaparlamentet, Rådet, Europeiska ekonomiska och sociala kommittén samt Regionkommittén. Handlingsplanen för e-hälsa 2012–2020 - Innovativ Hälsovård för det 21:a århundradet. /* COM/2012/0736 final */.

Rapporter, artiklar och dokument

Holm, H. Westring, E. (2015). NCS3: Informations- och styrsystem inom hälso- och sjukvård (FOI-R--4088--SE)

Myndigheten för samhällsskydd och beredskap, Den robusta sjukhusbyggnaden - 2020 En vägledning för funktionssäkra sjukhusfastigheter, Remissutgåva

Prop. 2016/17:43 En ny hälso- och sjukvårdslag

SOU 2013:2 Patientlag - Delbetänkande av Patientmaktsutredningen

SOU 2008:1177 Patientsäkerhet: Vad har gjorts? Vad behöver göras?

Webbsidor

Läkemedelsverkets föreskrifter - LVFS och HSLF-FS - https://www.lakemedelsverket.se/sv/lagar-och-regler/foreskrifter?q=medicintekniska%20produkter%20&c2=0.

Socialstyrelsen. En god och säker vård. https://patientsakerhet.socialstyrelsen.se/ledning-och-styrning/nationell-handlingsplan/en-god-och-saker-vard/

12.10 Reglering inom andra områden

Lagar

SFS 1949:105	Tryckfrihetsförordning
SFS 1962:700	Brottsbalk
SFS 1990:782	Arkivlag
SFS 2009:400	Offentlighets- och sekretesslag
SFS 2016:1145	Lag om offentlig upphandling
SFS 2016:116	Lag om upphandling inom försörjningssektorerna
SFS 2018:558	Lag om företagshemligheter

Förordningar

SFS 1991:446	Arkivförordning
SFS 2009:641	Offentlighets- och sekretessförordning

SFS 2016:1162 Upphandlingsförordning

EU direktiv och förordningar

Europaparlamentets och rådets direktiv 2016/943/EU av den 8 juni 2016 om skydd mot att icke röjd know-how och företagsinformation (företagshemligheter) olagligen anskaffas, utnyttjas och röjs

Rapporter, artiklar och dokument

Kommittédirektiv 2019:64, Säker och kostnadseffektiv it-drift för den offentliga förvaltningen

SOU 2021:1, Säker och kostnadseffektiv it-drift – rättsliga förutsättningar för utkontraktering

12.11 Ordlista

Webbsidor

https://www.lagrummet.se/lar-dig-mer/ordlistan-a-o#F

Security in Industrial Control Systems

Nationellt Centrum för säkerhet i styrsystem för samhällsviktig verksamhet (NCS3) är ett kompetenscentrum med uppdraget att bygga upp och sprida medvetenhet, kunskap och erfarenhet om cybersäkerhetsasspekter inom industriella informations- och styrsystem. Centrumets är ett samarbete mellan de svenska myndigheterna FOI och MSB och dess verksamhet fokuserar på aktörer som äger och/eller driver samhällsviktig verksamhet där industriella informations- och styrsystem ingår.

The National Centre for increased security in industrial control systems is a centre of excellence focused at building and disseminating awareness, knowledge and experience about cyber security aspects in ICS. The Centre is a cooperation between the Swedish Defence Research Agency and the Swedish Civil Contingencies Agency and the activities is focused on actors that owns and/or operates critical infrastructure where ICS are a part.

FOI
Swedish Defence Research Agency
SE-164 90 Stockholm

Phone +46 8 555 030 00
Fax +46 8 555 031 00

www.foi.se

Swedish Civil Contingencies Agency
SE-651 81 Karlstad

Phone: +46 (0) 771-240 240
Fax: +46 (0) 10-240 56 00

www.msb.se