DIN EN ISO/IEC 27019:2020-08 (D)

Informationstechnik - Sicherheitsverfahren - Informationssicherheitsmaßnahmen für die Energieversorgung (ISO/IEC 27019:2017, korrigierte Fassung 2019-08); Deutsche Fassung EN ISO/IEC 27019:2020

Inhalt

Seite

Europäisches Vorwort 6

Vorwort 7

0 Einleitung 9
0.1 Hintergrund und Kontext 9
0.2 Sicherheitsaspekte für Prozesssteuerungssysteme bei Energieversorgern 10
0.3 Anforderungen an Informationssicherheit 10
0.4 Auswahl der Maßnahmen 11
0.5 Zielgruppe 11

1 Anwendungsbereich 12

2 Normative Verweisungen 13

3 Begriffe 13

4 Aufbau dieses Dokuments 15
4.1 Allgemein 15
4.2 Anpassung der ISO/IEC 27001:2013-Anforderungen 15
4.3 Energieversorgungsspezifische Maßnahmen mit Bezug zu ISO/IEC 27002:2013 16

5 Informationssicherheitsrichtlinien 16

6 Organisation der Informationssicherheit 16
6.1 Interne Organisation 16
6.1.1 Informationssicherheitsrollen und -verantwortlichkeiten 16
6.1.2 Aufgabentrennung 16
6.1.3 Kontakt mit Behörden 16
6.1.4 Kontakt mit speziellen Interessensgruppen 17
6.1.5 Informationssicherheit im Projektmanagement 17
6.1.6 ENR - Identifizierung von Risiken in Zusammenhang mit Externen 17
6.1.7 ENR - Adressieren von Sicherheit im Umgang mit Kunden 18
6.2 Mobilgeräte und Telearbeit 18
6.2.1 Richtlinie zu Mobilgeräten 18
6.2.2 Telearbeit 19

7 Personalsicherheit 19
7.1 Vor der Beschäftigung 19
7.1.1 Sicherheitsüberprüfung 19
7.1.2 Beschäftigungs- und Vertragsbedingungen 20
7.2 Während der Beschäftigung 20
7.2.1 Verantwortlichkeiten der Leitung 20
7.2.2 Informationssicherheitsbewusstsein, -ausbildung und -schulung 20
7.2.3 Maßregelungsprozess 20
7.3 Beendigung und Änderung der Beschäftigung 20

8 Verwaltung der Werte 20
8.1 Verantwortlichkeit für Werte 20
8.1.1 Inventarisierung der Werte 20
8.1.2 Zuständigkeit für Werte 21

8.1.3 Zulässiger Gebrauch von Werten 21
8.1.4 Rückgabe von Werten 21
8.2 Informationsklassifizierung 21
8.2.1 Klassifizierung von Information 21
8.2.2 Kennzeichnung von Information 22
8.2.3 Handhabung von Werten 22
8.3 Handhabung von Datenträgern 22

9 Zugangssteuerung 22
9.1 Geschäftsanforderungen an die Zugangssteuerung 22
9.1.1 Zugangssteuerungsrichtlinie 22
9.1.2 Zugang zu Netzwerken und Netzwerkdiensten 23
9.2 Benutzerzugangsverwaltung 23
9.2.1 Registrierung und Deregistrierung von Benutzern 23
9.2.2 Zuteilung von Benutzerzugängen 23
9.2.3 Verwaltung privilegierter Zugangsrechte 23
9.2.4 Verwaltung geheimer Authentisierungsinformation von Benutzern 23
9.2.5 Überprüfung von Benutzerzugangsrechten 23
9.2.6 Entzug oder Anpassung von Zugangsrechten 23
9.3 Benutzerverantwortlichkeiten 24
9.3.1 Gebrauch geheimer Authentisierungsinformation 24
9.4 Zugangssteuerung für Systeme und Anwendungen 24
9.4.1 Informationszugangsbeschränkung 24
9.4.2 Sichere Anmeldeverfahren 24
9.4.3 System zur Verwaltung von Kennwörtern 24
9.4.4 Gebrauch von Hilfsprogrammen mit privilegierten Rechten 25
9.4.5 Zugangssteuerung für Quellcode von Programmen 25

10 Kryptographie 25
10.1 Kryptographische Maßnahmen 25
10.1.1 Richtlinie zum Gebrauch von kryptographischen Maßnahmen 25
10.1.2 Schlüsselverwaltung 25

11 Physische und umgebungsbezogene Sicherheit 25
11.1 Sicherheitsbereiche 25
11.1.1 Physische Sicherheitsperimeter 25
11.1.2 Physische Zutrittssteuerung 25
11.1.3 Sichern von Büros, Räumen und Einrichtungen 26
11.1.4 Schutz vor externen und umweltbedingten Bedrohungen 26
11.1.5 Arbeiten in Sicherheitsbereichen 26
11.1.6 Anlieferungs- und Ladebereiche 26
11.1.7 ENR — Sichern von Leitstellen 26
11.1.8 ENR — Sicherung von Technikräumen 27
11.1.9 ENR — Sicherung von Außenstandorten 28
11.2 Geräte und Betriebsmittel 29
11.2.1 Platzierung und Schutz von Geräten und Betriebsmitteln 29
11.2.2 Versorgungseinrichtungen 29
11.2.3 Sicherheit der Verkabelung 29
11.2.4 Instandhaltung von Geräten und Betriebsmitteln 29
11.2.5 Entfernen von Werten 30
11.2.6 Sicherheit von Geräten, Betriebsmitteln und Werten außerhalb der Räumlichkeiten 30
11.2.7 Sichere Entsorgung oder Wiederverwendung von Geräten und Betriebsmitteln 30
11.2.8 Unbeaufsichtigte Benutzergeräte 30
11.2.9 Richtlinie für eine aufgeräumte Arbeitsumgebung und Bildschirmsperren 30
11.3 ENR — Sicherheit in Räumlichkeiten Dritter 30
11.3.1 ENR — Betriebseinrichtung in Bereichen anderer Energieversorger 30
11.3.2 ENR - Betriebseinrichtung beim Kunden vor Ort 31
11.3.3 ENR — Gekoppelte Steuerungs- und Kommunikationssysteme 31

12 Betriebssicherheit 32

12.1 Betriebsabläufe und -verantwortlichkeiten 32
12.1.1 Dokumentierte Bedienabläufe 32
12.1.2 Änderungssteuerung 32
12.1.3 Kapazitätssteuerung 32
12.1.4 Trennung von Entwicklungs-, Test- und Betriebsumgebungen 32
12.2 Schutz vor Schadsoftware 33
12.2.1 Maßnahmen gegen Schadsoftware 33
12.3 Datensicherung 33
12.4 Protokollierung und Überwachung 33
12.4.1 Ereignisprotokollierung 33
12.4.2 Schutz der Protokollinformation 33
12.4.3 Administratoren- und Bedienerprotokolle 33
12.4.4 Uhrensynchronisation 34
12.5 Steuerung von Software im Betrieb 34
12.5.1 Installation von Software auf Systemen im Betrieb 34
12.6 Handhabung technischer Schwachstellen 34
12.6.1 Handhabung von technischen Schwachstellen 34
12.6.2 Einschränkungen von Softwareinstallation 34
12.7 Audits von Informationssystemen 35
12.8 ENR — Altsysteme 35
12.8.1 ENR — Behandlung von Altsystemen 35
12.9 ENR - Safety-Funktionen 35
12.9.1 ENR — Integrität und Verfügbarkeit von Safety-Funktionen 36

13 Kommunikationssicherheit 36
13.1 Netzwerksicherheitsmanagement 36
13.1.1 Netzwerksteuerungsmaßnahmen 36
13.1.2 Sicherheit von Netzwerkdiensten 36
13.1.3 Trennung in Netzwerken 36
13.1.4 ENR — Sicherung der Prozessdatenkommunikation 37
13.1.5 ENR — Logische Anbindung von externen Prozesssteuerungssystemen 37
13.2 Informationsübertragung 38

14 Anschaffung, Entwicklung und Instandhaltung von Systemen 38
14.1 Sicherheitsanforderungen an Informationssysteme 38
14.1.1 Analyse und Spezifikation von Informationssicherheitsanforderungen 38
14.1.2 Sicherung von Anwendungsdiensten in öffentlichen Netzwerken 38
14.1.3 Schutz der Transaktionen bei Anwendungsdiensten 38
14.2 Sicherheit in Entwicklungs- und Unterstützungsprozessen 38
14.2.1 Richtlinie für sichere Entwicklung 38
14.2.2 Verfahren zur Verwaltung von Systemänderungen 38
14.2.3 Technische Überprüfung von Anwendungen nach Änderungen an der Betriebsplattform 38
14.2.4 Beschränkung von Änderungen an Softwarepaketen 39
14.2.5 Grundsätze für die Analyse, Entwicklung und Pflege sicherer Systeme 39
14.2.6 Sichere Entwicklungsumgebung 39
14.2.7 Ausgegliederte Entwicklung 39
14.2.8 Testen der Systemsicherheit 39
14.2.9 Systemabnahmetest 39
14.2.10 ENR — Least Functionality 39
14.3 Testdaten 39

15 Lieferantenbeziehungen 40
15.1 Informationssicherheit in Lieferantenbeziehungen 40
15.1.1 Informationssicherheitsrichtlinie für Lieferantenbeziehungen 40
15.1.2 Behandlung von Sicherheit in Lieferantenvereinbarungen 40
15.1.3 Lieferkette für Informations- und Kommunikationstechnologie 40
15.2 Steuerung der Dienstleistungserbringung von Lieferanten 40

16 Handhabung von Informationssicherheitsvorfällen 40
16.1 Handhabung von Informationssicherheitsvorfällen und -verbesserungen 40

16.1.1 Verantwortlichkeiten und Verfahren 40
16.1.2 Meldung von Informationssicherheitsereignissen 40
16.1.3 Meldung von Schwächen in der Informationssicherheit 40
16.1.4 Beurteilung von und Entscheidung über Informationssicherheitsereignisse 41
16.1.5 Reaktion auf Informationssicherheitsvorfälle 41
16.1.6 Erkenntnisse aus Informationssicherheitsvorfällen 41
16.1.7 Sammeln von Beweismaterial 41

17 Informationssicherheitsaspekte beim Business Continuity Management 41
17.1 Aufrechterhalten der Informationssicherheit 41
17.2 Redundanzen 41
17.2.1 Verfügbarkeit von informationsverarbeitenden Einrichtungen 41
17.2.2 ENR — Notfallkommunikation 42

18 Compliance 43
18.1 Einhaltung gesetzlicher und vertraglicher Anforderungen 43
18.1.1 Bestimmung der anwendbaren Gesetzgebung und der vertraglichen Anforderungen 43
18.1.2 Geistige Eigentumsrechte 43
18.1.3 Schutz von Aufzeichnungen 43
18.1.4 Privatsphäre und Schutz von personenbezogener Information 43
18.1.5 Regelungen bezüglich kryptographischer Maßnahmen 43
18.2 Überprüfungen der Informationssicherheit 44
18.2.1 Unabhängige Überprüfung der Informationssicherheit 44
18.2.2 Einhaltung von Sicherheitsrichtlinien und –standards 44
18.2.3 Überprüfung der Einhaltung von technischen Vorgaben 44

Anhang A (normativ) Energieversorgungs-spezifische Referenzmaßnahmenziele und Maßnahmen 45

Literaturhinweise 48