DIN EN ISO/IEC 27019:2026-03 (D)

Informationssicherheit, Cybersicherheit und Schutz der Privatsphäre - Informationssicherheitsmaßnahmen für die Energieversorgung (ISO/IEC 27019:2024); Deutsche Fassung EN ISO/IEC 27019:2025

Inhalt

Seite

Europäisches Vorwort 7
Vorwort 8
Einleitung 9
1 Anwendungsbereich 12
2 Normative Verweisungen 12
3 Begriffe und Abkürzungen 13
3.1 Begriffe 13
3.2 Abkürzungen 15
4 Aufbau dieses Dokuments 15
5 Organisatorische Maßnahmen 15
5.1 Informationssicherheitspolitik und -richtlinien 15
5.2 Informationssicherheitsrollen und -verantwortlichkeiten 16
5.3 Aufgabentrennung 16
5.4 Verantwortlichkeiten der Leitung 16
5.5 Kontakt mit Behörden 16
5.6 Kontakt mit speziellen Interessengruppen 17
5.7 Informationen über die Bedrohungslage 17
5.8 Informationssicherheit im Projektmanagement 17
5.9 Inventar der Informationen und anderer damit verbundener Werte 17
5.10 Zulässiger Gebrauch von Informationen und anderen damit verbundenen Werten 18
5.11 Rückgabe von Werten 18
5.12 Klassifizierung von Informationen 18
5.13 Kennzeichnung von Information 19
5.14 Informationsübermittlung 19
5.15 Zugangssteuerung 19
5.16 Identitätsmanagement 20
5.17 Authentisierungsinformationen 20
5.18 Zugangsrechte 21
5.19 Informationssicherheit in Lieferantenbeziehungen 21
5.20 Behandlung von Informationssicherheit in Lieferantenvereinbarungen 21
5.21 Umgang mit der Informationssicherheit in der IKT-Lieferkette 21
5.22 Überwachung, Überprüfung und Änderungsmanagement von Lieferantendienstleistungen 21
5.23 Informationssicherheit für die Nutzung von Cloud-Diensten 22
5.24 Planung und Vorbereitung der Handhabung von Informationssicherheitsvorfällen 22
5.25 Beurteilung und Entscheidung über Informationssicherheitsereignisse 22
5.26 Reaktion auf Informationssicherheitsvorfälle 22
5.27 Erkenntnisse aus Informationssicherheitsvorfällen 22
5.28 Sammeln von Beweismaterial 22
5.29 Informationssicherheit bei Störungen 22
5.30 IKT-Bereitschaft für Business-Continuity 22
5.31 Juristische, gesetzliche, regulatorische und vertragliche Anforderungen 22
5.32 Geistige Eigentumsrechte 23

5.33 Schutz von Aufzeichnungen ... 23
5.34 Datenschutz und Schutz personenbezogener Daten (pbD) ... 23
5.35 Unabhängige Überprüfung der Informationssicherheit ... 23
5.36 Einhaltung von Richtlinien, Vorschriften und Normen für die Informationssicherheit ... 23
5.37 Dokumentierte Betriebsabläufe ... 23
5.38 ENR — Identifizierung von Risiken in Zusammenhang mit externen Geschäftspartnern ... 23
5.39 ENR — Adressieren von Sicherheit im Umgang mit Kunden ... 24

6 Personenbezogene Maßnahmen ... 25
6.1 Sicherheitsüberprüfung ... 25
6.2 Beschäftigungs- und Vertragsbedingungen ... 25
6.3 Informationssicherheitsbewusstsein, -ausbildung und -schulung ... 26
6.4 Maßregelungsprozess ... 26
6.5 Verantwortlichkeiten bei Beendigung oder Änderung der Beschäftigung ... 26
6.6 Vertraulichkeits- oder Geheimhaltungsvereinbarungen ... 26
6.7 Remote-Arbeit ... 26
6.8 Meldung von Informationssicherheitsereignissen ... 27

7 Physische Maßnahmen ... 27
7.1 Physische Sicherheitsperimeter ... 27
7.2 Physischer Zutritt ... 27
7.3 Sichern von Büros, Räumen und Einrichtungen ... 27
7.4 Physische Sicherheitsüberwachung ... 27
7.5 Schutz vor physischen und umweltbedingten Bedrohungen ... 27
7.6 Arbeiten in Sicherheitsbereichen ... 27
7.7 Aufgeräumte Arbeitsumgebung und Bildschirmsperren ... 27
7.8 Platzierung und Schutz von Geräten und Betriebsmitteln ... 28
7.9 Sicherheit von Werten außerhalb der Räumlichkeiten ... 28
7.10 Speichermedien ... 29
7.11 Versorgungseinrichtungen ... 29
7.12 Sicherheit der Verkabelung ... 29
7.13 Instandhaltung von Geräten und Betriebsmitteln ... 29
7.14 Sichere Entsorgung oder Wiederverwendung von Geräten und Betriebsmitteln ... 29
7.15 ENR — Sicherung von Leitstellen ... 30
7.16 ENR — Sicherung von Technikräumen ... 31
7.17 ENR — Sicherung von Außenstandorten ... 32
7.18 ENR — Gekoppelte Steuerungs- und Kommunikationssysteme ... 33

8 Technologische Maßnahmen ... 34
8.1 Endpunktgeräte des Benutzers ... 34
8.2 Privilegierte Zugangsrechte ... 35
8.3 Informationszugangsbeschränkung ... 35
8.4 Zugriff auf den Quellcode ... 35
8.5 Sichere Authentisierung ... 35
8.6 Kapazitätssteuerung ... 35
8.7 Schutz gegen Schadsoftware ... 35
8.8 Handhabung von technischen Schwachstellen ... 36
8.9 Konfigurationsmanagement ... 36
8.10 Löschung von Informationen ... 36
8.11 Datenmaskierung ... 36
8.12 Verhinderung von Datenlecks ... 37
8.13 Sicherung von Informationen ... 37
8.14 Redundanz von informationsverarbeitenden Einrichtungen ... 37
8.15 Protokollierung ... 37
8.16 Überwachung von Aktivitäten ... 37
8.17 Uhrensynchronisation ... 38
8.18 Gebrauch von Hilfsprogrammen mit privilegierten Rechten ... 38
8.19 Installation von Software auf Systemen in Betrieb ... 38
8.20 Netzwerksicherheit ... 38

8.21 Sicherheit von Netzwerkdiensten ... 38
8.22 Trennung von Netzwerken ... 39
8.23 Webfilterung ... 39
8.24 Verwendung von Kryptographie ... 39
8.25 Lebenszyklus einer sicheren Entwicklung ... 39
8.26 Anforderungen an die Anwendungssicherheit ... 39
8.27 Sichere Systemarchitektur und Entwicklungsgrundsätze ... 39
8.28 Sichere Codierung ... 39
8.29 Sicherheitsprüfung bei Entwicklung und Abnahme ... 39
8.30 Ausgegliederte Entwicklung ... 40
8.31 Trennung von Entwicklungs-, Test- und Produktionsumgebungen ... 40
8.32 Änderungssteuerung ... 40
8.33 Testdaten ... 40
8.34 Schutz der Informationssysteme während Tests im Rahmen von Audits ... 40
8.35 ENR — Behandlung von Altsystemen (Legacy-Systemen) ... 40
8.36 ENR — Integrität und Verfügbarkeit von Safety-Funktionen ... 41
8.37 ENR — Sicherung der Prozessdatenkommunikation ... 42
8.38 ENR — Logische Anbindung von externen Prozesssteuerungssystemen ... 43
8.39 ENR — Least Functionality ... 44
8.40 ENR — Notfallkommunikation ... 45

Anhang A (informativ) Verweisung auf energieversorgungsspezifische Maßnahmen ... 47

Anhang B (informativ) Übereinstimmung zwischen diesem Dokument und der ersten Ausgabe (ISO/IEC 27019:2017) ... 49

Literaturhinweise ... 62

Tabellen

Tabelle A.1 — Energieversorgungsspezifische Sicherheitsmaßnahmen ... 47

Tabelle B.1 — Übereinstimmung zwischen Maßnahmen in diesem Dokument und Maßnahmen in ISO/IEC 27019:2017 ... 49

Tabelle B.2 — Übereinstimmung zwischen Maßnahmen in ISO/IEC 27019:2017 und Maßnahmen in diesem Dokument ... 54