

# DIN ISO/IEC TR 27019:2015-03 (D)

## Informationstechnik - Sicherheitsverfahren - Leitfaden für das Informationssicherheitsmanagement von Steuerungssystemen der Energieversorgung auf Grundlage der ISO/IEC 27002 (ISO/IEC TR 27019:2014)

---

Inhalt	Seite
Nationales Vorwort.....	6
Nationaler Anhang NA (informativ) Literaturhinweise .....	7
Einleitung .....	8
1 Anwendungsbereich .....	10
2 Normative Verweisungen .....	10
3 Begriffe .....	11
4 Übersicht .....	12
4.1 Aufbau dieser Norm .....	12
4.2 Informationssicherheits-Managementsysteme im Bereich der Energieversorgung .....	13
4.2.1 Zielsetzung .....	13
4.2.2 Sicherheitsbetrachtungen für Prozesssteuerungssysteme der Energieversorgung .....	13
4.2.3 Schützenswerte Informationswerte .....	13
4.2.4 Aufbau eines Informationssicherheits-Managements .....	14
4.2.5 Entscheidende Erfolgsfaktoren .....	14
5 Sicherheitsleitlinie .....	14
6 Organisation der Informationssicherheit .....	15
6.1 Interne Organisation .....	15
6.1.1 Engagement des Managements für Informationssicherheit .....	15
6.1.2 Koordination der Informationssicherheit .....	15
6.1.3 Zuweisung der Verantwortlichkeiten für Informationssicherheit .....	15
6.1.4 Genehmigungsverfahren für informationsverarbeitende Einrichtungen .....	15
6.1.5 Vertraulichkeitsvereinbarungen .....	15
6.1.6 Kontakt zu Behörden .....	15
6.1.7 Kontakt zu speziellen Interessensgruppen .....	16
6.1.8 Unabhängige Überprüfung der Informationssicherheit .....	16
6.2 Externe .....	16
6.2.1 Identifizierung von Risiken in Zusammenhang mit externen Mitarbeitern .....	16
6.2.2 Adressieren von Sicherheit im Umgang mit Kunden .....	16
6.2.3 Adressieren von Sicherheit in Vereinbarungen mit Dritten .....	17
7 Management von organisationseigenen Werten .....	17
7.1 Verantwortung für organisationseigene Werte (Assets) .....	17
7.1.1 Inventar der organisationseigenen Werte (Assets) .....	17
7.1.2 Eigentum von organisationseigenen Werten (Assets) .....	18
7.1.3 Zulässiger Gebrauch von organisationseigenen Werten (Assets) .....	18
7.2 Klassifizierung von Informationen .....	18
7.2.1 Regelung für die Klassifizierung .....	18
7.2.2 Kennzeichnung von und Umgang mit Informationen .....	19
8 Personalsicherheit .....	19
8.1 Vor der Anstellung .....	19
8.1.1 Aufgaben und Verantwortlichkeiten .....	19
8.1.2 Überprüfung .....	19
8.1.3 Arbeitsvertragsklauseln .....	19
8.2 Während der Anstellung .....	20
8.3 Beendigung oder Änderung der Anstellung .....	20

9	Physische und umgebungsbezogene Sicherheit.....	20
9.1	Sicherheitsbereiche.....	20
9.1.1	Sicherheitszonen.....	20
9.1.2	Zutrittskontrolle.....	20
9.1.3	Sicherung von Büros, Räumen und Einrichtungen.....	20
9.1.4	Schutz vor Bedrohungen von außen und aus der Umgebung.....	20
9.1.5	Arbeiten in Sicherheitszonen.....	20
9.1.6	Öffentlicher Zugang, Anlieferungs- und Ladezonen.....	20
9.1.7	Sichern von Leitstellen.....	20
9.1.8	Sicherung von Technikräumen.....	21
9.1.9	Sicherung von Außenstandorten.....	23
9.2	Sicherheit von Betriebsmitteln.....	23
9.2.1	Platzierung und Schutz von Betriebsmitteln.....	23
9.2.2	Unterstützende Versorgungseinrichtungen.....	24
9.2.3	Sicherheit der Verkabelung.....	24
9.2.4	Instandhaltung von Gerätschaften.....	24
9.2.5	Sicherheit von außerhalb des Standorts befindlicher Ausrüstung.....	24
9.2.6	Sichere Entsorgung oder Weiterverwendung von Betriebsmitteln.....	24
9.2.7	Entfernung von Eigentum.....	24
9.3	Sicherheit in Räumlichkeiten Dritter.....	24
9.3.1	Betriebseinrichtung in Bereichen anderer Energieversorger.....	25
9.3.2	Betriebseinrichtung beim Kunden vor Ort.....	25
9.3.3	Gekoppelte Steuerungs- und Kommunikationssysteme.....	26
10	Betriebs- und Kommunikationsmanagement.....	26
10.1	Verfahren und Verantwortlichkeiten.....	26
10.1.1	Dokumentierte Betriebsprozesse.....	26
10.1.2	Änderungsverwaltung.....	26
10.1.3	Aufteilung der Verantwortlichkeiten.....	26
10.1.4	Trennung von Entwicklungs-, Test- und Produktiveinrichtungen.....	26
10.2	Management der Dienstleistungserbringung von Dritten.....	27
10.3	Systemplanung und Abnahme.....	27
10.4	Schutz vor Schadsoftware und mobilem Programmcode.....	27
10.4.1	Maßnahmen gegen Schadsoftware.....	27
10.4.2	Schutz vor mobiler Software (mobile Agenten).....	28
10.5	Backup.....	28
10.6	Management der Netzsicherheit.....	28
10.6.1	Maßnahmen für Netze.....	28
10.6.2	Sicherheit von Netzdiensten.....	28
10.6.3	Sicherung der Prozessdatenkommunikation.....	28
10.7	Handhabung von Speicher- und Aufzeichnungsmedien.....	29
10.8	Austausch von Informationen.....	29
10.9	E-Commerce-Anwendungen.....	29
10.10	Überwachung.....	29
10.10.1	Auditprotokolle.....	29
10.10.2	Überwachung der Systemnutzung.....	29
10.10.3	Schutz von Protokollinformationen.....	29
10.10.4	Administrator- und Betreiberprotokolle.....	29
10.10.5	Fehlerprotokolle.....	29
10.10.6	Zeitsynchronisation.....	29
10.11	Altsysteme.....	30
10.11.1	Behandlung von Altsystemen.....	30
10.12	Betriebssicherheit.....	30
10.12.1	Integrität und Verfügbarkeit von Funktionen der Betriebssicherheit.....	31
11	Zugangskontrolle.....	31
11.1	Geschäftsanforderungen für Zugangskontrolle.....	31
11.1.1	Leitlinie zur Zugangskontrolle.....	31
11.2	Benutzerverwaltung.....	31
11.3	Benutzerverantwortung.....	31
11.3.1	Passwortverwendung.....	31
11.3.2	Unbeaufsichtigte Benutzerausstattung.....	32
11.3.3	Der Grundsatz des aufgeräumten Schreibtischs und des leeren Bildschirms.....	32

11.4	Zugangskontrolle für Netze .....	32
11.4.1	Regelwerk zur Nutzung von Netzdiensten .....	32
11.4.2	Benutzerauthentisierung für externe Verbindungen .....	32
11.4.3	Geräteidentifikation in Netzen .....	32
11.4.4	Schutz der Diagnose- und Konfigurationsports .....	32
11.4.5	Trennung in Netzen .....	32
11.4.6	Kontrolle von Netzverbindungen .....	33
11.4.7	Routingkontrolle für Netze .....	33
11.4.8	Logische Anbindung von externen Prozesssteuerungssystemen .....	33
11.5	Zugriffskontrolle auf Betriebssysteme .....	33
11.5.1	Verfahren für sichere Anmeldung .....	33
11.5.2	Benutzeridentifikation und Authentisierung .....	33
11.5.3	Systeme zur Verwaltung von Passwörtern .....	34
11.5.4	Verwendung von Systemwerkzeugen .....	34
11.5.5	Session Time-out .....	34
11.5.6	Begrenzung der Verbindungszeit .....	34
11.6	Zugangskontrolle zu Anwendungen und Information .....	34
11.7	Mobile Computing und Telearbeit .....	34
12	Beschaffung, Entwicklung und Wartung von Informationssystemen .....	34
12.1	Sicherheitsanforderungen von Informationssystemen .....	34
12.1.1	Analyse und Spezifikation von Sicherheitsanforderungen .....	34
12.2	Korrekte Verarbeitung in Anwendungen .....	34
12.3	Kryptographische Maßnahmen .....	35
12.4	Sicherheit von Systemdateien .....	35
12.4.1	Kontrolle von Software im Betrieb .....	35
12.4.2	Schutz von Test-Daten .....	35
12.4.3	Zugangskontrolle zu Quellcode .....	35
12.5	Sicherheit bei Entwicklungs- und Unterstützungsprozessen .....	35
12.6	Umgang mit Schwachstellen .....	35
13	Umgang mit Informationssicherheitsvorfällen .....	35
13.1	Melden von Informationssicherheitsereignissen und Schwachstellen .....	35
13.2	Umgang mit Informationssicherheitsvorfällen und Verbesserungen .....	35
14	Sicherstellung des Geschäftsbetriebs (Business Continuity Management) .....	36
14.1	Informationssicherheitsaspekte bei der Sicherstellung des Geschäftsbetriebs (Business Continuity Management) .....	36
14.1.1	Einbeziehung der Informationssicherheit in den Prozess zur Sicherstellung des Geschäftsbetriebs .....	36
14.1.2	Sicherstellung des Geschäftsbetriebs und Risikoeinschätzung .....	36
14.1.3	Entwickeln und Umsetzen von Plänen zur Sicherstellung des Geschäftsbetriebs, die Informationssicherheit enthalten .....	36
14.1.4	Rahmenwerk für die Pläne zur Sicherstellung des Geschäftsbetriebs .....	36
14.1.5	Testen, Instandhaltung und Neubewertung von Plänen zur Sicherstellung des Geschäftsbetriebs .....	36
14.2	Wesentliche Notfalldienste .....	36
14.2.1	Notfall-Kommunikation .....	36
15	Einhaltung von Vorgaben (Compliance) .....	37
15.1	Einhaltung gesetzlicher Vorgaben .....	37
15.1.1	Identifikation der anwendbaren Gesetze .....	37
15.1.2	Rechte an geistigem Eigentum .....	38
15.1.3	Schutz von organisationseigenen Aufzeichnungen .....	38
15.1.4	Datenschutz und Vertraulichkeit von personenbezogenen Informationen .....	38
15.1.5	Verhinderung des Missbrauchs von informationsverarbeitenden Einrichtungen .....	38
15.1.6	Leitlinien zu kryptographischen Verfahren .....	38
15.2	Einhaltung von Sicherheitsleitlinien und -standards, und technischer Vorgaben .....	38
15.3	Überlegungen zu Revisionsprüfungen von Informationssystemen .....	38
	Anhang A (informativ) Erweiterter Maßnahmenkatalog für die Energieversorgung .....	39
	Anhang B (informativ) Zusätzliche Umsetzungsempfehlungen .....	42
	Literaturhinweise .....	52