

DIN SPEC 27009:2012-04 (D)

Leitfaden für das Informationssicherheitsmanagement von Steuerungssystemen der Energieversorgung auf Grundlage der ISO/IEC 27002

| Inhalt | Seite |
|--|-------|
| Vorwort | 4 |
| Einleitung | 4 |
| 1 Anwendungsbereich | 7 |
| 2 Normative Verweisungen | 7 |
| 3 Begriffe | 7 |
| 4 Übersicht | 9 |
| 4.1 Aufbau dieser Norm | 9 |
| 4.2 Informationssicherheits-Managementsysteme im Bereich der Energieversorgung | 10 |
| 5 Sicherheitsleitlinie | 11 |
| 6 Organisation der Informationssicherheit | 11 |
| 6.1 Interne Organisation | 11 |
| 6.2 Externe | 13 |
| 7 Management von organisationseigenen Werten | 14 |
| 7.1 Verantwortung für organisationseigene Werte (Assets) | 14 |
| 7.2 Klassifizierung von Informationen | 15 |
| 8 Personalsicherheit | 15 |
| 8.1 Vor der Anstellung | 15 |
| 8.2 Während der Anstellung | 16 |
| 8.3 Beendigung oder Änderung der Anstellung | 16 |
| 9 Physische und umgebungsbezogene Sicherheit | 16 |
| 9.1 Sicherheitsbereiche | 16 |
| 9.2 Sicherheit von Betriebsmitteln | 19 |
| 9.3 Sicherheit in Räumlichkeiten Dritter | 21 |
| 10 Betriebs- und Kommunikationsmanagement | 22 |
| 10.1 Verfahren und Verantwortlichkeiten | 22 |
| 10.2 Management der Dienstleistungserbringung von Dritten | 23 |
| 10.3 Systemplanung und Abnahme | 23 |
| 10.4 Schutz vor Schadsoftware und mobilem Programmcode | 23 |
| 10.5 Backup | 24 |
| 10.6 Management der Netzsicherheit | 24 |
| 10.7 Handhabung von Speicher- und Aufzeichnungsmedien | 25 |
| 10.8 Austausch von Informationen | 25 |
| 10.9 E-Commerce-Anwendungen | 25 |
| 10.10 Überwachung | 25 |
| 10.11 Altsysteme | 26 |
| 10.12 Betriebssicherheit | 26 |
| 11 Zugangskontrolle | 27 |
| 11.1 Geschäftsanforderungen für Zugangskontrolle | 27 |
| 11.2 Benutzerverwaltung | 27 |

| | | |
|------|--|----|
| 11.3 | Benutzerverantwortung | 27 |
| 11.4 | Zugangskontrolle für Netze | 28 |
| 11.5 | Zugriffskontrolle auf Betriebssysteme | 29 |
| 11.6 | Zugangskontrolle zu Anwendungen und Information | 30 |
| 11.7 | Mobile Computing und Telearbeit | 30 |
| 12 | Beschaffung, Entwicklung und Wartung von Informationssystemen | 30 |
| 12.1 | Sicherheitsanforderungen von Informationssystemen | 30 |
| 12.2 | Korrekte Verarbeitung in Anwendungen | 30 |
| 12.3 | Kryptographische Maßnahmen | 30 |
| 12.4 | Sicherheit von Systemdateien | 31 |
| 12.5 | Sicherheit bei Entwicklungs- und Unterstützungsprozessen | 31 |
| 12.6 | Umgang mit Schwachstellen | 31 |
| 13 | Umgang mit Informationssicherheitsvorfällen | 31 |
| 13.1 | Melden von Informationssicherheitsereignissen und Schwachstellen | 31 |
| 13.2 | Umgang mit Informationssicherheitsvorfällen und Verbesserungen | 31 |
| 14 | Sicherstellung des Geschäftsbetriebs (Business Continuity Management) | 31 |
| 14.1 | Informationssicherheitsaspekte bei der Sicherstellung des Geschäftsbetriebs (Business Continuity Management) | 31 |
| 14.2 | Wesentliche Notfalldienste | 32 |
| 15 | Einhaltung von Vorgaben (Compliance) | 33 |
| 15.1 | Einhaltung gesetzlicher Vorgaben | 33 |
| 15.2 | Einhaltung von Sicherheitsleitlinien und -standards, und technischer Vorgaben | 34 |
| 15.3 | Überlegungen zu Revisionsprüfungen von Informationssystemen | 34 |
| | Anhang A (informativ) Erweiterter Maßnahmenkatalog für die Energieversorgung | 35 |
| | Anhang B (informativ) Zusätzliche Umsetzungsempfehlungen | 38 |
| | Literaturhinweise | 48 |