

E DIN EN ISO/IEC 27017:2025-03 (D/E)

Erscheinungsdatum: 2025-02-21

Informationssicherheit, Cybersicherheit und Schutz der Privatsphäre -
Informationssicherheitsmaßnahmen auf der Grundlage von ISO/IEC 27002 für Cloud-
Dienste (ISO/IEC DIS 27017:2025); Deutsche und Englische Fassung prEN ISO/IEC
27002:2025

Information security, cybersecurity and privacy protection - Information security
controls based on ISO/IEC 27002 for cloud services (ISO/IEC DIS 27017:2025);
German and English version prEN ISO/IEC 27002:2025

| Inhalt | Seite |
|---|-------|
| Europäisches Vorwort..... | 8 |
| Vorwort..... | 9 |
| Einleitung..... | 11 |
| 1 Anwendungsbereich..... | 12 |
| 2 Normative Verweisungen..... | 12 |
| 3 Begriffe und Abkürzungen..... | 12 |
| 3.1 Begriffe..... | 12 |
| 3.2 Abkürzungen..... | 12 |
| 4 Spezifische Konzepte des Cloud Computing..... | 13 |
| 4.1 Allgemein..... | 13 |
| 4.1.1 Überblick..... | 13 |
| 4.1.2 Gliederung dieser Internationalen Norm..... | 14 |
| 4.2 Spezifische Konzepte des Cloud Computing..... | 14 |
| 4.2.1 Lieferantenbeziehungen bei Cloud-Diensten..... | 14 |
| 4.2.2 Beziehungen zwischen CSCs und CSPs..... | 15 |
| 4.2.3 Umgang mit Informationssicherheitsrisiken bei Cloud-Diensten..... | 16 |
| 5 Spezifische Anleitungen für Cloud-Dienste in Zusammenhang mit organisatorischen Maßnahmen..... | 16 |
| 5.1 Informationssicherheitsrichtlinien..... | 16 |
| 5.2 Informationssicherheitsrollen und -verantwortlichkeiten..... | 18 |
| 5.3 Aufgabentrennung..... | 18 |
| 5.4 Verantwortlichkeiten der Leitung..... | 18 |
| 5.5 Kontakt mit Behörden..... | 19 |
| 5.6 Kontakt mit speziellen Interessengruppen..... | 19 |
| 5.7 Bedrohungsdaten..... | 19 |
| 5.8 Informationssicherheit im Projektmanagement..... | 19 |
| 5.9 Inventar der Informationen und anderen damit verbundenen Werten..... | 19 |
| 5.10 Zulässige Verwendung von Informationen und anderen damit verbundenen Werten..... | 20 |
| 5.11 Rückgabe von Werten..... | 20 |
| 5.12 Klassifizierung von Information..... | 21 |
| 5.13 Kennzeichnung von Information..... | 21 |
| 5.14 Informationsübertragung..... | 21 |
| 5.15 Zugangssteuerung..... | 21 |
| 5.16 Identitätsverwaltung..... | 21 |
| 5.17 Authentifizierungsinformationen..... | 22 |
| 5.18 Zugangsrechte..... | 22 |
| 5.19 Informationssicherheit in Lieferantenbeziehungen..... | 22 |

| | | |
|------|--|-----------|
| 5.20 | Behandlung von Informationssicherheit in Lieferantenvereinbarungen | 22 |
| 5.21 | Umgang mit der Informationssicherheit in der IKT-Lieferkette | 23 |
| 5.22 | Überwachung, Überprüfung und Änderungsmanagement von Lieferantendienstleistungen | 24 |
| 5.23 | Informationssicherheit für die Nutzung von Cloud-Diensten..... | 24 |
| 5.24 | Planung und Vorbereitung der Handhabung von Informationssicherheitsvorfällen | 24 |
| 5.25 | Beurteilung und Entscheidung über Informationssicherheitsereignisse | 26 |
| 5.26 | Reaktion auf Informationssicherheitsvorfälle | 26 |
| 5.27 | Erkenntnisse aus Informationssicherheitsvorfällen..... | 26 |
| 5.28 | Sammeln von Beweismaterial..... | 27 |
| 5.29 | Informationssicherheit bei Störungen..... | 27 |
| 5.30 | IKT-Bereitschaft für Business Continuity..... | 27 |
| 5.31 | Identifizierung von rechtlichen, gesetzlichen, regulatorischen und vertraglichen Anforderungen..... | 27 |
| 5.32 | Geistige Eigentumsrechte | 29 |
| 5.33 | Schutz von Aufzeichnungen | 29 |
| 5.34 | Datenschutz und Schutz personenbezogener Daten (pBD)..... | 29 |
| 5.35 | Unabhängige Überprüfung der Informationssicherheit..... | 30 |
| 5.36 | Einhaltung von Richtlinien und Normen für die Informationssicherheit..... | 30 |
| 5.37 | Dokumentierte Betriebsabläufe..... | 30 |
| 6 | Spezifische Anleitungen für Cloud-Dienste in Zusammenhang mit personenbezogenen Maßnahmen | 31 |
| 6.1 | Sicherheitsüberprüfung..... | 31 |
| 6.2 | Beschäftigungs- und Vertragsbedingungen..... | 31 |
| 6.3 | Informationssicherheitsbewusstsein, -ausbildung und -schulung..... | 31 |
| 6.4 | Maßregelungsprozess..... | 32 |
| 6.5 | Verantwortlichkeiten nach Beendigung oder Änderung des Beschäftigungsverhältnisses..... | 32 |
| 6.6 | Vertraulichkeits- oder Geheimhaltungsvereinbarungen..... | 32 |
| 6.7 | Telearbeit | 32 |
| 6.8 | Meldung von Informationssicherheitsereignissen | 32 |
| 7 | Spezifische Anleitungen für Cloud-Dienste in Zusammenhang mit personenbezogenen Maßnahmen | 33 |
| 7.1 | Physische Sicherheitsperimeter | 33 |
| 7.2 | Physische Zutrittssteuerung..... | 33 |
| 7.3 | Sicherung von Büros, Räumen und Einrichtungen..... | 33 |
| 7.4 | Physische Sicherheitsüberwachung..... | 33 |
| 7.5 | Schutz vor physischen und umweltbedingten Bedrohungen | 33 |
| 7.6 | Arbeit in Sicherheitsbereichen..... | 33 |
| 7.7 | Aufgeräumte Arbeitsumgebung und Bildschirmsperren..... | 34 |
| 7.8 | Platzierung und Schutz von Geräten und Betriebsmitteln | 34 |
| 7.9 | Sicherheit von Werten außerhalb der Räumlichkeiten..... | 34 |
| 7.10 | Speichermedien | 34 |
| 7.11 | Versorgungseinrichtungen | 34 |
| 7.12 | Sicherheit der Verkabelung..... | 34 |
| 7.13 | Instandhaltung von Geräten und Betriebsmitteln | 34 |
| 7.14 | Sichere Entsorgung oder Wiederverwendung von Geräten und Betriebsmitteln | 34 |
| 8 | Spezifische Anleitungen für Cloud-Dienste in Zusammenhang mit technologischen Maßnahmen | 35 |
| 8.1 | Endpunktgeräte des Benutzers | 35 |
| 8.2 | Privilegierte Zugangsrechte | 35 |
| 8.3 | Informationszugangsbeschränkung | 35 |
| 8.4 | Zugriff auf den Quellcode..... | 36 |
| 8.5 | Sichere Authentifizierung..... | 36 |
| 8.6 | Kapazitätssteuerung | 36 |
| 8.7 | Schutz gegen Schadsoftware..... | 37 |
| 8.8 | Handhabung von technischen Schwachstellen..... | 37 |

| | | |
|---|---|----|
| 8.9 | Konfigurationsmanagement..... | 37 |
| 8.10 | Löschung von Informationen..... | 38 |
| 8.11 | Datenmaskierung..... | 39 |
| 8.12 | Verhinderung von Datenlecks..... | 39 |
| 8.13 | Sicherung von Information | 39 |
| 8.14 | Verfügbarkeit von informationsverarbeitenden Einrichtungen..... | 40 |
| 8.15 | Protokollierung..... | 40 |
| 8.16 | Überwachungstätigkeiten | 41 |
| 8.17 | Uhrensynchronisation | 42 |
| 8.18 | Gebrauch von Hilfsprogrammen mit privilegierten Rechten | 42 |
| 8.19 | Installation von Software auf Betriebssystemen | 42 |
| 8.20 | Netzwerksteuerungsmaßnahmen | 42 |
| 8.21 | Sicherheit von Netzwerkdiensten..... | 43 |
| 8.22 | Trennung in Netzwerken | 43 |
| 8.23 | Webfilterung..... | 43 |
| 8.24 | Verwendung von Kryptographie..... | 43 |
| 8.25 | Sicherer Entwicklungslebenszyklus..... | 44 |
| 8.26 | Anforderungen an die Anwendungssicherheit..... | 45 |
| 8.27 | Grundsätze für die Architektur, Analyse, Entwicklung und Pflege sicherer Systeme..... | 45 |
| 8.28 | Sichere Programmierung..... | 45 |
| 8.29 | Sicherheitsprüfung bei Entwicklung und Abnahme | 45 |
| 8.30 | Ausgegliederte Entwicklung..... | 45 |
| 8.31 | Trennung von Entwicklungs-, Test- und Produktionsumgebungen..... | 45 |
| 8.32 | Änderungssteuerung..... | 45 |
| 8.33 | Testinformationen | 46 |
| 8.34 | Schutz von Informationssystemen bei Audits und Tests..... | 46 |
| Anhang A (normativ) Erweiterungssatz von Maßnahmen für Cloud-Dienste..... | | 47 |
| Anhang B (informativ) Übereinstimmung mit ISO/IEC 27017:2015 | | 52 |
| Anhang C (informativ) Überwachung von Cloud-Diensten | | 59 |
| Literaturhinweise | | 61 |

Tabellen

| | |
|--|----|
| Tabelle B.1 — Übereinstimmung zwischen Maßnahmen in diesem Dokument und ISO/IEC 27017:2015 | 52 |
| Tabelle B.2 — Übereinstimmung zwischen Maßnahmen in ISO/IEC 27017:2015 und diesem Dokument..... | 56 |