ZERTIFIKAT ◆ CERTIFICATE ◆ 認證證書 ◆ СЕРТИФИКАТ ◆ CERTIFICADO ◆ CERTIFICAT

Management Service

ZERTIFIKAT

Die Zertifizierungsstelle
der TÜV SÜD Management Service GmbH

bescheinigt, dass das Unternehmen

PlusServer GmbH
Hohenzollernring 72
50672 Köln
Deutschland

für den Geltungsbereich

Bereitstellung und Betrieb von
Rechenzentrumskapazitäten, Netzwerkanbindungen
sowie des Service 'Cloud Connect'

einschließlich der Standorte und Geltungsbereiche
gemäß Anlage

ein Informationssicherheitsmanagementsystem
gemäß „Erklärung zur Anwendbarkeit“ eingeführt hat und anwendet.

Durch ein Audit, Auftrags-Nr. **70775393**,
wurde der Nachweis erbracht, dass die Forderungen der

ISO/IEC 27001:2013

erfüllt sind.

Dieses Zertifikat ist gültig vom **01.06.2020** bis **31.05.2023**.

Zertifikat-Registrier-Nr.: **12 310 40834 TMS**.

Version der Erklärung zur Anwendbarkeit: **3.2; 2020-01-04**.

Leiter der Zertifizierungsstelle
München, 31.03.2021

DAkkS Deutsche Akkreditierungsstelle D-ZM-14143-01-00

TÜV SÜD Management Service GmbH • Zertifizierungsstelle • Ridlerstrasse 57 • 80339 München • Germany
www.tuev-sued.de/certificate-validity-check

ZERTIFIKAT ◆ CERTIFICATE ◆ 認證證書 ◆ СЕРТИФИКАТ ◆ CERTIFICADO ◆ CERTIFICAT

Management Service

Anlage zur Zertifizierungsurkunde Nr.: 12 310 40834 TMS

Standorte	Geltungsbereich
PlusServer GmbH Hohenzollernring 72 50672 Köln Deutschland	Bereitstellung und Betrieb von Rechenzentrumskapazitäten, Netzwerkanbindungen sowie des Service 'Cloud Connect'.
PlusServer GmbH Altmarkt 25 01067 Dresden Deutschland	Bereitstellung und Betrieb von Rechenzentrumskapazitäten, Netzwerkanbindungen sowie des Service 'Cloud Connect'.
PlusServer GmbH In der Steele 33a-41 40599 Düsseldorf Deutschland	Bereitstellung und Betrieb von Rechenzentrumskapazitäten, Netzwerkanbindungen sowie des Service 'Cloud Connect'.
PlusServer GmbH An der Autobahn 200 33333 Gütersloh Deutschland	Bereitstellung und Betrieb von Rechenzentrumskapazitäten, Netzwerkanbindungen sowie des Service 'Cloud Connect'.
PlusServer GmbH Verler Straße 6 33332 Gütersloh Deutschland	Bereitstellung und Betrieb von Rechenzentrumskapazitäten, Netzwerkanbindungen sowie des Service 'Cloud Connect'.
PlusServer GmbH Essener Bogen 17 22419 Hamburg Deutschland	Bereitstellung und Betrieb von Rechenzentrumskapazitäten, Netzwerkanbindungen sowie des Service 'Cloud Connect'.
PlusServer GmbH Nagelsweg 33-35 20097 Hamburg Deutschland	Bereitstellung und Betrieb von Rechenzentrumskapazitäten, Netzwerkanbindungen sowie des Service 'Cloud Connect'.
PlusServer GmbH König-Georg-Deich 21107 Hamburg-Wilhelmsburg Deutschland	Bereitstellung und Betrieb von Rechenzentrumskapazitäten, Netzwerkanbindungen sowie des Service 'Cloud Connect'.
PlusServer GmbH Welserstraße 14 51149 Köln Deutschland	Bereitstellung und Betrieb von Rechenzentrumskapazitäten, Netzwerkanbindungen sowie des Service 'Cloud Connect'.
PlusServer GmbH Heidbergstraße 101-111 22846 Norderstedt Deutschland	Bereitstellung und Betrieb von Rechenzentrumskapazitäten, Netzwerkanbindungen sowie des Service 'Cloud Connect'.

Leiter der Zertifizierungsstelle
München, 31.03.2021

DAkkS Deutsche Akkreditierungsstelle D-ZM-14143-01-00

TÜV SÜD Management Service GmbH • Zertifizierungsstelle • Ridlerstrasse 57 • 80339 München • Germany
www.tuev-sued.de/certificate-validity-check

ISO 27001:2013 - Statement of Applicabilty

plusserver

Nr.	Anforderung ISO 27001:2013	Beschreibung der Anforderung	Anwendbar	Status	Begründung der Nicht-/Anwendbarkeit
A.5	Sicherheitsleitlinien				
A.5.1	Vorgaben der Leitung zur Informationssicherheit Ziel: Bereitstellung von Vorgaben und Unterstützung seitens der Leitung für die Informationssicherheit nach geschäftlichen Anforderungen und den geltenden Gesetzen und Vorschriften.				
A.5.1.1	Informationssicherheitsleitlinien	Ein Satz Informationssicherheitsleitlinien ist festzulegen, von der Leitung zu genehmigen, zu veröffentlichen und den Mitarbeitern sowie relevanten externen Parteien bekanntzumachen.	ja	100%	Geschäftliche Anforderung
A.5.1.2	Prüfung der Informationssicherheitsleitlinie	Die Informationssicherheitsleitlinien müssen in planmäßigen Abständen oder jeweils nach erheblichen Änderungen geprüft werden, um sicherzustellen, dass sie nach wie vor geeignet, angemessen und wirksam sind.	ja	100%	Geschäftliche Anforderung
A.6	Organisation der Informationssicherheit				
A.6.1	Interne Organisation Ziel: Festlegung eines Frameworks für die Leitung, mit dem die Implementierung der Informationssicherheit in der Organisation eingeleitet und kontrolliert werden kann.				
A.6.1.1	Aufgaben und Zuständigkeiten im Bereich der Informationssicherheit	Alle Zuständigkeiten im Bereich der Informationssicherheit müssen festgelegt und zugeordnet werden.	ja	100%	Geschäftliche Anforderung
A.6.1.2	Aufgabentrennung (Aufteilung von Verantwortlichkeiten)	Miteinander in Konflikt stehende Aufgaben und Zuständigkeitsbereiche müssen getrennt werden, um das Risiko unautorisierter oder versehentlicher Änderungen oder missbräuchlicher Anwendung der Werte der Organisation zu verringern.	ja	100%	Geschäftliche Anforderung Gesetzliche Vorgabe
A.6.1.3	Kontakt zu Behörden	Es sind angemessene Kontakte zu relevanten Behörden zu pflegen.	ja	100%	Geschäftliche Anforderung Gesetzliche Vorgabe
A.6.1.4	Kontakt mit Interessen- Vertretungen	Es sind angemessene Kontakte zu Interessenvertretungen oder sonstigen sicherheitsorientierten Expertenforen und Fachverbänden zu pflegen.	ja	100%	Geschäftliche Anforderung
A.6.1.5	Informationssicherheit im Projektmanagement	Die Informationssicherheit muss ungeachtet der Art des Projekts auch im Projektmanagement berücksichtigt werden.	ja	100%	Geschäftliche Anforderung
A.6.2	Mobilgeräte und Telearbeit Ziel: Sicherstellung der Informationssicherheit bei Telearbeit und der Nutzung von Mobilgeräten				
A.6.2.1	Leitlinie zu Mobilgeräten	Es müssen eine Leitlinie und unterstützende Sicherheitsmaßnahmen zum Schutz vor den Risiken durch die Nutzung von Mobilgeräten eingesetzt werden.	ja	100%	Geschäftliche Anforderung
A.6.2.2	Telearbeit	Es müssen eine Leitlinie und unterstützende Sicherheitsmaßnahmen zum Schutz von Informationen festgelegt werden, auf die von Telearbeitsplätzen aus zugegriffen wird oder die dort verarbeitet oder gespeichert werden.	nein	out of scope	Die PlusServer betreibt keine Telearbeitsplätze gemäß § 2 Abs. 7 ArbStättV.
A.7	Sicherheit des Personals				
A.7.1	Vor der Einstellung Ziel: Festlegung eines Frameworks für die Leitung, mit dem die Implementierung der Informationssicherheit in der Organisation eingeleitet und kontrolliert werden kann				
A.7.1.1	Überprüfung	Prüfung des Hintergrunds von Bewerbern müssen im Einklang mit den relevanten Gesetzen, Vorschriften und ethischen Grundsätzen sowie in einem angemessenen Verhältnis zu den geschäftlichen Anforderungen, der Einstufung der einzuholenden Informationen und den wahrgenommenen Risiken stehen.	ja	100%	Geschäftliche Anforderung Gesetzliche Vorgabe

Nr.	Anforderung ISO 27001:2013	Beschreibung der Anforderung	Anwendbar	Status	Begründung der Nicht-/Anwendbarkeit
A.7.1.2	Arbeitsvertragsklauseln	Im Rahmen ihrer vertraglichen Verpflichtung müssen Mitarbeiter den Arbeitsvertragsklauseln in ihrem Arbeitsvertrag, mit denen ihre eigenen Pflichten und die Pflichten der Organisation im Bereich der Informationssicherheit festgelegt werden, zustimme und sie unterzeichnen.	ja	100%	Geschäftliche Anforderung Gesetzliche Vorgabe
A.7.2	Während der Anstellung Ziel: Sicherstellung, dass Mitarbeiter und externe Benutzer ihre Pflichten bezüglich der Informationssicherheit kennen und ihnen nachkommen.				
A.7.2.1	Verantwortung des Managements	Das Management muss alle Mitarbeiter und externen Benutzer dazu anhalten, Sicherheitsmaßnahmen entsprechend den festgelegten Leitlinien und Verfahren der Organisation anzuwen	ja	100%	Geschäftliche Anforderung
A.7.2.2	Bewusstsein, Ausbildung und Schulur für Informationssicherheit	Alle Mitarbeiter der Organisation sowie, falls relevant, externe Benutzer müssen ein Programm zur Sensibilisierung für Informationssicherheit sowie entsprechende Aus- und Weiterbildung und Schulungen durchlaufen und regelmäßig bezüglich der Leitlinien und Verfahren der Organisation, die für ihre berufliche Funktion relevant sind, auf dem neusten Stand gehalten werden.	ja	100%	Geschäftliche Anforderung Gesetzliche Vorgabe
A.7.2.3	Disziplinarverfahren	Es muss ein formales und offiziell bekanntgegebenes Disziplinarverfahren eingeleitet werden, in dessen Rahmen Maßnahmen gegen Mitarbeiter verhängt werden können, die gegen Informationssicherheitsvorschriften verstoßen haben.	ja	100%	Geschäftliche Anforderung
A.7.3	Beendigung und Wechsel der Anstellung Ziel: Schutz der Interessen der Organisation bei einem Wechsel oder der Beendigung der Anstellung				
A.7.3.1	Zuständigkeiten bei Beendigung oder Wechsel der Anstellung	Zuständigkeiten und Pflichten im Bereich der Informationssicherheit, die auch nach Beendigung oder Wechse der Anstellung gültig bleiben, müssen definiert, dem Mitarbeiter oder externen Benutzer mitgeteilt und durchgesetzt werden.	ja	100%	Geschäftliche Anforderung
A.8	Wertemanagement				
A.8.1	Verantwortung der Werte Ziel: Erreichen und Erhaltung eines angemessenen Schutzes der Werte der Organisation				
A.8.1.1	Inventar Werte	Werte, die mit Informationen und Einrichtung zur Verarbeitung v Informationen in Zusammenhang stehen, müssen ermittelt werden, und von diesen Anlagen ist ein Inventar zu erstellen un zu pflegen.	ja	100%	Geschäftliche Anforderung
A.8.1.2	Eigentum von Werten	Für im Inventar geführte Werte muss es Eigentümer geben.	ja	100%	Geschäftliche Anforderung
A.8.1.3	Zulässiger Gebrauch von Werten	Es müssen Regeln für den zulässigen Gebrauch von Informationen und Werten, die mit Informationen und Einrichtungen zur Verarbeitung von Informationen in Zusammenhang stehen, aufgestellt, dokumentiert und implementiert werden.	ja	100%	Geschäftliche Anforderung
A.8.1.4	Rückgabe von Werten	Alle Mitarbeiter und externen Benutzer müssen sämtliche Werte der Organisation zurückgeben, die sich bei Auslauf ihrer Anstellung oder ihres Vertrags noch in ihrem Besitz befinden.	ja	100%	Geschäftliche Anforderung
A.8.2	Klassifizierung von Informationen Ziel: Sicherstellung, dass Informationen eine angemessene Schutzstufe entsprechend ihrer Bedeutung für die Organisation zugeteilt bekommen.				
A.8.2.1	Klassifizierung von Informationen	Informationen sind nach ihrem Wert, gesetzlichen Anforderunge Vertraulichkeit und Betriebswichtigkeit zu klassifizieren.	ja	100%	Geschäftliche Anforderung
A.8.2.2	Kennzeichnung von Informationen	Ein angemessener Satz Verfahren zur Kennzeichnung von Informationen ist entsprechend dem von der Organisation eingesetzten Plan zur Einstufung von Informationen zu entwicke und zu implementieren.	ja	100%	Geschäftliche Anforderung

Nr.	Anforderung ISO 27001:2013	Beschreibung der Anforderung	Anwendbar	Status	Begründung der Nicht-/Anwendbarkeit
A.8.2.3	Umgang mit Werten	Verfahren für den Umgang mit Werten sind entsprechend dem v der Organisation eingesetzten Plan zur Einstufung von Informationen zu entwickeln und zu implementieren.	ja	100%	Geschäftliche Anforderung
A.8.3	Umgang mit Medien Ziel: Verhinderung von unerlaubter Veröffentlichung, Veränderung, Entnahme oder Zerstörung von Informationen, die auf Medien gespeichert sind				
A.8.3.1	Verwaltung von Wechselmedien	Es sind Verfahren für die Verwaltung von Wechselmedien entsprechend dem von der Organisation eingesetzten Plan zur Klassifizierung von Informationen zu implementieren.	ja	100%	Geschäftliche Anforderung
A.8.3.2	Entsorgung von Medien	Medien müssen sicher und unter Anwendung formaler Verfahrensanweisungen entsorgt werden, wenn sie nicht mehr benötigt werden.	ja	100%	Geschäftliche Anforderung Gesetzliche Vorgabe
A.8.3.3	Physische Weitergabe von Medien	Medien, auf denen Informationen gespeichert sind, müssen vor unautorisiertem Zugriff, missbräuchlicher Verwendung oder Verfälschung während des Transports geschützt werden.	ja	100%	Geschäftliche Anforderung Gesetzliche Vorgabe
A.9	Zugriffskontrolle				
A.9.1	Geschäftliche Anforderungen in Bezug auf die Zugriffskontrolle Ziel: Beschränkung des Zugriffs auf Informationen und informationsverarbeitenden Einrichtungen				
A.9.1.1	Zugriffskontrollleitlinie	Eine Zugriffskontrollleitlinie ist auf Grundlage der geschäftlichen und sicherheitsrelevanten Anforderungen zu erstellen, zu dokumentieren und zu prüfen.	ja	100%	Geschäftliche Anforderung
A.9.1.2	Leitlinie zur Nutzung von Netzwerkdiensten	Benutzer dürfen ausschließlich auf denjenigen Netzwerken und Netzwerkdiensten Zugriff erhalten, zu deren Nutzung sie ausdrücklich autorisiert wurden.	ja	100%	Geschäftliche Anforderung
A.9.2	Benutzerverwaltung Ziel: Sicherstellung des Zugriffs ausschließlich für autorisierte Benutzer und Verhinderung von nicht autorisierten Zugriffen auf Systeme und Dienste.				
A.9.2.1	An- und Abmeldung von Benutzern	Es muss ein formales Verfahren für die An- und Abmeldung von Benutzern implementiert werden, mit dem allen Arten von Benutzern der Zugriff auf Systeme und Dienste gewährt und wieder entzogen werden kann.	ja	100%	Geschäftliche Anforderung
A.9.2.2	Vergabe von Benutzerrechten	Die Zuordnung von geheimen Authentisierungsinformationen muss über einen formalen Verwaltungsprozess kontrolliert werden.	ja	100%	Geschäftliche Anforderung
A.9.2.3	Verwaltung von Sonderrechten	Die Zuteilung und Nutzung von Sonderzugriffsrechten muss eingeschränkt und kontrolliert werden.	ja	100%	Geschäftliche Anforderung
A.9.2.4	Verwaltung geheimer Authentisierungsinformationen von Benutzern	Die Zuordnung von geheimen Authentisierungsinformationen muss über einen formalen Verwaltungsprozess kontrolliert werden.	ja	100%	Geschäftliche Anforderung
A.9.2.5	Prüfung von Zugriffsberechtigungen der Benutzer	Werteeigentümer müssen die Zugriffsberechtigungen der Benutzer in regelmäßigen Abständen prüfen.	ja	100%	Geschäftliche Anforderung
A.9.2.6	Entzug oder Anpassung von Zugriffsberechtigungen	Die Zugriffsberechtigungen aller Mitarbeiter und externen Benutzer zu Informationen und informationsverarbeitenden Einrichtungen müssen nach Auslauf der Anstellung oder des Vertrags entzogen bzw. bei einem Wechsel der Anstellung entsprechend angepasst werden.	ja	100%	Geschäftliche Anforderung
A.9.3	Benutzerverantwortung Ziel: Übertragung der Verantwortung für den Schutz der Authentisierungsinformationen auf die Benutzer				
A.9.3.1	Verwendung von geheimen Authentisierungsinformationen	Von den Benutzern muss verlangt werden, die sicherheitsrelevanten Praktiken der Organisation zur Verwendur von geheimen Authentisierungsinformationen zu befolgen.	ja	100%	Geschäftliche Anforderung
A.9.4	Kontrolle des Zugriffs auf Systeme und Anwendungen Ziel: Verhinderung des unautorisierten Zugriffs auf Systeme und Anwendungen				
A.9.4.1	Beschränkung des Zugriffs auf Informationen	Der Zugriff auf Funktionen von Informations- und Anwendungssystemen muss entsprechend der Zugriffskontrollleitlinie beschränkt werden.	ja	100%	Geschäftliche Anforderung
A.9.4.2	Sichere Anmeldeverfahren	Der Zugriff auf Systeme und Anwendungen muss über ein sicheres Anmeldeverfahren kontrolliert werden, wenn dies nach der Zugriffskontrollleitlinie erforderlich ist.	ja	100%	Geschäftliche Anforderung

Nr.	Anforderung ISO 27001:2013	Beschreibung der Anforderung	Anwendbar	Status	Begründung der Nicht-/Anwendbarkeit
A.9.4.3	Kennwortmanagementsystem	Kennwortmanagementsysteme müssen interaktiv sein und stark Kennwörter erfordern.	ja	100%	Geschäftliche Anforderung
A.9.4.4	Verwendung von Dienstprogrammen mit Sonderberechtigungen	Die Verwendung von Dienstprogrammen, mit denen sich u. U. System- und Anwendungskontrollen umgehen lassen, muss beschränkt und streng kontrolliert werden.	ja	100%	Geschäftliche Anforderung
A.9.4.5	Kontrolle des Zugriffs auf Software-Quellcode	Der Zugriff auf den Software-Quellcode muss beschränkt werden.	ja	100%	Geschäftliche Anforderung
A.10	Kryptographie				
A.10.1	Kryptographische Maßnahmen Ziel: Sicherstellung der ordnungsnahen und wirksamen Verwendung von Kryptographie zum Schutz der Vertraulichkeit, Authentizität oder Integrität von Informationen				
A.10.1.1	Leitlinie zur Nutzung von kryptographischen Maßnahmen	Eine Leitlinie zur Verwendung von kryptographischen Maßnahm für den Schutz von Informationen ist zu entwickeln und zu implementieren.	ja	100%	Geschäftliche Anforderung Gesetzliche Vorgabe
A.10.1.2	Verwaltung von Schlüsseln	Eine Leitlinie zur Verwendung, zum Schutz und zur Gültigkeitsdauer von kryptographischen Schlüsseln ist zu entwickeln und über deren gesamte Nutzungsdauer hinweg umzusetzen.	ja	100%	Geschäftliche Anforderung Gesetzliche Vorgabe
A.11	Schutz vor physischem Zugang und Umwelteinflüssen				
A.11.1	Sicherheitsbereiche Ziel: Verhinderung des unautorisierten physischen Zugriffs auf die Informationen und informationsverarbeitende Einrichtungen der Organisation sowie deren Beschädigung und Beeinträchtigung.				
A.11.1.1	Physische Sicherheitszone	Zum Schutz von Bereichen, in denen sich entweder vertrauliche oder betriebswichtige Informationen oder informationsverarbeitende Einrichtungen befinden, sind Sicherheitszonen festzulegen und zu verwenden.	ja	100%	Geschäftliche Anforderung
A.11.1.2	Physische Zugangskontrolle	Sicherheitsbereiche müssen durch angemessene Zugriffskontrollen geschützt werden, durch die sichergestellt ist, dass nur autorisiertes Personal Zutritt hat.	ja	100%	Geschäftliche Anforderung
A.11.1.3	Sicherung von Zweigstellen, Räumen und Anlagen	Es sind physische Sicherungsvorkehrungen für Niederlassungen Räume und Anlagen zu konzipieren und anzuwenden.	ja	100%	Geschäftliche Anforderung
A.11.1.4	Schutz vor externen und umweltbedingten Bedrohungen	Es sind physische Schutzvorkehrungen gegen Naturkatastrophe vorsätzliche Angriffe oder Unfälle zu konzipieren und anzuwend	ja	100%	Geschäftliche Anforderung
A.11.1.5	Arbeit in Sicherheitsbereichen	Es sind physische Schutzvorkehrungen und Richtlinien für die Arbeit in Sicherheitsbereichen zu konzipieren und anzuwenden.	ja	100%	Geschäftliche Anforderung
A.11.1.6	Anlieferungs- und Ladezonen	Zugangspunkte wie Anlieferungs- und Ladezonen sowie andere Punkte, über die sich unautorisierte Personen Zugang zu den Betriebsgebäuden verschaffen könnten, müssen kontrolliert und nach Möglichkeit von informationsverarbeitenden Einrichtungen isoliert werden, um unautorisierten Zugriff zu verhindern.	ja	100%	Geschäftliche Anforderung
A.11.2	Betriebsmittel Ziel: Vorbeugung von Verlust, Beschädigung, Diebstahl oder Beeinträchtigung von Werten und Unterbrechungen der Betriebstätigkeit der Organisation				
A.11.2.1	Platzierung und Schutz von Betriebsmitteln	Betriebsmittel sind so zu platzieren und zu schützen, dass Risik durch Umweltbedrohungen und Gefährdungen sowie Möglichkeiten für den unautorisierten Zugriff verringert werden.	ja	100%	Geschäftliche Anforderung
A.11.2.2	Versorgungseinrichtungen	Betriebsmittel müssen vor Stromausfällen und anderen Betriebsunterbrechungen durch Ausfälle von Versorgungseinrichtungen geschützt werden.	ja	100%	Geschäftliche Anforderung
A.11.2.3	Sicherheit der Verkabelung	Stromversorgungs- und Telekommunikationskabel, die zur Übertragung von Daten oder zur Unterstützung von Informationsdiensten verwendet werden, sind vor dem Abfange der Daten sowie vor Beeinträchtigung oder Beschädigung zu schützen.	ja	100%	Geschäftliche Anforderung

Nr.	Anforderung ISO 27001:2013	Beschreibung der Anforderung	Anwendbar	Status	Begründung der Nicht-/Anwendbarkeit
A.11.2.4	Instandhaltung von Gerätschaften	Gerätschaften müssen ordnungsnach instand gehalten und gep werden, um ihre Verfügbarkeit und Integrität sicherzustellen.	ja	100%	Geschäftliche Anforderung
A.11.2.5	Entfernung von Werten	Ausstattung, Informationen oder Software dürfen nicht ohne vorherige Autorisierung vom Standort entfernt werden.	ja	100%	Geschäftliche Anforderung
A.11.2.6	Sicherheit von Betriebsmitteln und Werten außerhalb der Betriebsgebäud	Sicherheitsvorkehrungen werden unter Berücksichtigung der diversen Risiken bei Arbeiten außerhalb der Betriebsgebäude d Organisation auch auf Werte außerhalb des Standorts angewan	ja	100%	Geschäftliche Anforderung
A.11.2.7	Sichere Entsorgung oder Wiederverwendung von Betriebsmitte	Alle Geräte, die Speichermedien enthalten, müssen vor ihrer Entsorgung oder Wiederverwendung überprüft werden, um sicherzustellen, dass vertrauliche Daten und lizenzierte Softwar entfernt oder sicher überschrieben wurden.	ja	100%	Geschäftliche Anforderung
A.11.2.8	Unbeaufsichtigte Benutzerausstattung	Benutzer müssen sicherstellen, dass unbeaufsichtigte Ausstattu angemessen geschützt ist.	ja	100%	Geschäftliche Anforderung
A.11.2.9	Der Grundsatz des aufgeräumten Schreibtischs und des leeren Bildschirms	Der Grundsatz des aufgeräumten Schreibtisches für Papiere un Wechselmedien sowie des leeren Bildschirms für informationsverarbeitende Einrichtungen muss Anwendung find	ja	100%	Geschäftliche Anforderung
A.12	Betriebssicherheit				
A.12.1	Betriebsverfahren und Zuständigkeiten Ziel: Sicherstellung des ordnungsnahen und sicheren Betriebs von Vorrichtungen zur Verarbeitung von Informationen				
A.12.1.1	Dokumentierte Betriebsverfahren	Die Betriebsverfahren müssen dokumentiert und allen Benutzer zugänglich gemacht werden, die sie benötigen.	ja	100%	Geschäftliche Anforderung
A.12.1.2	Änderungsmanagement	Änderungen an der Organisation, an Geschäftsprozessen, an Datenverarbeitungseinrichtungen und an Systemen sind zu kontrollieren.	ja	100%	Geschäftliche Anforderung
A.12.1.3	Kapazitätsmanagement	Die Ressourcennutzung muss überwacht und abgestimmt werden, und es sind Prognosen zu zukünftigen Kapazitätsanforderungen zu erstellen, um ausreichende Systemleistung sicherzustellen.	ja	100%	Geschäftliche Anforderung
A.12.1.4	Trennung von Entwicklungs-, Test- und Betriebsumgebungen	Entwicklungs-, Test- und Betriebsumgebungen sind zu trennen, um das Risiko unautorisierter Zugriffe oder unautorisierter Änderungen an der Betriebsumgebung zu verringern.	ja	100%	Geschäftliche Anforderung
A.12.2	Schutz vor Malware Ziel: Sicherstellung, dass Daten und Datenverarbeitungseinrichtungen vor Malware geschützt sind				
A.12.2.1	Kontrollmaßnahmen gegen Malware	Es sind Erkennungs-, Präventions- und Wiederherstellungsmaßnahmen zum Schutz von Malware in Verbindung mit einer angemessenen Sensibilisierung der Benutzer zu implementieren.	ja	100%	Geschäftliche Anforderung
A.12.3	Datensicherungen Ziel: Schutz vor Datenverlust				
A.12.3.1	Datensicherung	Es sind Sicherungskopien von Daten und Software sowie syste Images anzufertigen und regelmäßig entsprechend der vereinbarten Sicherungsleitlinie zu prüfen.	ja	100%	Geschäftliche Anforderung Gesetzliche Vorgabe
A.12.4	Protokollierung und Überwachung Ziel: Aufzeichnung von Ereignissen und Generierung von Beweismaterial				
A.12.4.1	Ereignisprotokollierung	Es sind Ereignisprotokolle anzufertigen, aufzubewahren und regelmäßig zu prüfen, in denen Aktivitäten der Benutzer, Ausnahmen, Fehler und Informationssicherheitsereignisse aufgezeichnet werden.	ja	100%	Geschäftliche Anforderung
A.12.4.2	Schutz von Protokollinformationen	Protokollierungseinrichtungen und Protokollinformationen müsse vor Manipulation und unbefugtem Zugriff geschützt werden.	ja	100%	Geschäftliche Anforderung

Nr.	Anforderung ISO 27001:2013	Beschreibung der Anforderung	Anwendbar	Status	Begründung der Nicht-/Anwendbarkeit
A.12.4.3	Administrator- und Betreiberprotokolle	Es sind Protokolle der Aktivitäten von Systemadministratoren ur Systembetreibern anzufertigen, zu schützen und regelmäßig zu prüfen.	ja	100%	Geschäftliche Anforderung
A.12.4.4	Zeitsynchronisation	Die Uhren aller relevanten Datenverarbeitungssysteme innerhal einer Organisation oder einer Sicherheitsdomäne müssen auf ei einzelne Referenz-Zeitquelle synchronisiert werden.	ja	100%	Geschäftliche Anforderung
A.12.5	Kontrolle von Software im Betrieb Ziel: Sicherstellung der Integrität von Systemen im Betrieb				
A.12.5.1	Installation von Software auf Systeme im Betrieb	Es sind Verfahren zur Kontrolle der Installation von Software au betriebsrelevanten Systemen zu implementieren	ja	100%	Geschäftliche Anforderung
A.12.6	Management technischer Schwachstellen Ziel: Verhinderung einer Ausnutzung technischer Schwachstellen				
A.12.6.1	Management technischer Schwachstellen	Informationen über technische Schwachstellen von verwendeter Informationssystemen müssen rechtzeitig eingeholt werden, die Anfälligkeit der Organisation für eine Ausnutzung solcher Schwachstellen ist zu bewerten, und es müssen angemessene Maßnahmen für den Umgang mit dem damit einhergehenden Risiko ergriffen werden.	ja	100%	Geschäftliche Anforderung
A.12.6.2	Beschränkungen der Software-Installation	Für Software-Installation durch Benutzer müssen Regeln festgelegt und implementiert werden.	ja	100%	Geschäftliche Anforderung
A.12.7	Auswirkungen von Audits auf Informationssysteme Ziel: Minimierung der Auswirkungen von Audit-Aktivitäten auf Systeme im Betrieb				
A.12.7.1	Kontrollen für Audits von Informationssystemen	Audit-Anforderungen und- Aktivitäten im Zusammenhang mit betriebsrelevanten Systemen müssen sorgfältig geplant und vereinbart werden, um Unterbrechungen der Geschäftsabläufe z minimieren.	ja	100%	Geschäftliche Anforderung
A.13	Sicherheit in der Kommunikation				
A.13.1	Netzwerksicherheitsmanagement Ziel: Sicherstellung des Schutzes von Informationen in Netzwerken und den unterstützenden informationsverarbeitenden Einrichtungen				
A.13.1.1	Netzwerkkontrollen	Netzwerke müssen verwaltet und kontrolliert werden, um Informationen in Systemen und Anwendungen zu schützen	ja	100%	Geschäftliche Anforderung
A.13.1.2	Sicherheit von Netzwerkdiensten	Es müssen Sicherheitsmechanismen, Service-Level und Anforderungen für die Verwaltung aller Netzwerkdienste aufgenommen werden, und zwar unabhängig davon, ob diese Dienste intern erbracht oder ausgelagert werden.	ja	100%	Geschäftliche Anforderung
A.13.1.3	Trennung in Netzwerken	Gruppen von Informationsdiensten, Benutzern und Informationssystemen müssen in Netzwerken voneinander getrennt gehalten werden.	ja	100%	Geschäftliche Anforderung Gesetzliche Vorgabe
A.13.2	Informationsübertragung Ziel: Wahrung der Sicherheit von Informationen, die innerhalb einer Organisation oder im Austausch mit einer externen Stelle übertragen werden.				
A.13.2.1	Leitlinien und Verfahren für die Informationsübertragung	Es müssen formale Leitlinien, Verfahren und Kontrollmaßnahme in Kraft sein, mit denen die Informationsübertragung über alle Arten von Kommunikationseinrichtungen geschützt wird.	ja	100%	Geschäftliche Anforderung
A.13.2.2	Vereinbarung zur Informationsübertragung	Es muss Vereinbarungen für die sichere Übertragung von geschäftlichen Informationen zwischen der Organisation und externen Partnern.	ja	100%	Geschäftliche Anforderung
A.13.2.3	Elektronische Nachrichten-Übermittlung	Es müssen formale Leitlinien, Verfahren und Kontrollmaßnahme in Kraft sein, mit denen die Informationsübertragung über alle Arten von Kommunikationseinrichtungen geschützt wird.	ja	100%	Geschäftliche Anforderung
A.13.2.4	Vertraulichkeits- oder Geheimhaltungsvereinbarungen	Entsprechend den Bedürfnissen der Organisation in Bezug auf d Schutz von Informationen müssen Anforderungen für Vertraulichkeits- oder Geheimhaltungsvereinbarungen ermittelt, regelmäßig geprüft und dokumentiert werden.	ja	100%	Geschäftliche Anforderung Gesetzliche Vorgabe

Nr.	Anforderung ISO 27001:2013	Beschreibung der Anforderung	Anwendbar	Status	Begründung der Nicht-/Anwendbarkeit
A.14	Anschaffung, Entwicklung und Instandhaltung von Systemen				
A.14.1	Sicherheitsanforderungen für Informationssysteme Ziel: Sicherstellung, dass Sicherheit über den gesamten Lebenszyklus von Informationssystemen hinweg fester Bestandteil dieser Systeme ist. Dies beinhaltet insbesondere spezifische Sicherheitsanforderungen für Informationssysteme, mit denen Dienste über öffentliche Netze bereitgestellt werden.				
A.14.1.1	Analyse und Spezifikation von Sicherheitsanforderungen	Die Anforderungen für Kontrollen der Informationssicherheit müssen in den Angaben zu den geschäftlichen und technischen Anforderungen für neue Informationssysteme oder Verbesserungen an bestehenden Informationssystemen enthalt sein, und darin müssen alle relevanten Kriterien wie die gesamte Nutzungsdauer oder ggf. die Verfügbarkeit der Anwendung übe öffentliche Netze berücksichtigt sein.	ja	100%	Geschäftliche Anforderung
A.14.1.2	Sicherung von Anwendungsdiensten i öffentlichen Netzen	Informationen im Zusammenhang mit Anwendungsdiensten, die über öffentliche Netze übertragen werden, müssen gegen betrügerische Aktivitäten, Vertragsstreitigkeiten, unberechtigte Veröffentlichung oder Veränderung geschützt werden.	nein	out of scope	Der Geltungsbereich der Zertifizierung umfasst keine Anwendungsdienste die Informationen über öffentliche Netze übertragen. Der Geltungsbereich wurde absichtlich so gewählt, da die Vielzahl möglicher Anwendungsdienste eine individuelle Betrachtung (pro Kunde) benötigt.
A.14.1.3	Schutz von Transaktionen im Zusammenhang mit Anwendungsdiensten	Informationen, die im Zuge von Transaktionen im Zusammenha mit Anwendungsdiensten übertragen werden, müssen geschütz werden, um unvollständigen Übertragungen und Fehlleitungen sowie unautorisierten Offenlegungen, Vervielfältigungen oder wiederholten Wiedergabe von Nachrichten vorzubeugen.	nein	out of scope	Der Geltungsbereich der Zertifizierung umfasst keine Anwendungsdienste die Informationen über öffentliche Netze übertragen. Der Geltungsbereich wurde absichtlich so gewählt, da die Vielzahl möglicher Anwendungsdienste eine individuelle Betrachtung (pro Kunde) benötigt.
A.14.2	Sicherheit in Entwicklungs- und Unterstützungsprozessen Ziel: Sicherstellung, dass Informationssicherheit im Rahmen des Entwicklungszyklus von Informationssystemen konzipiert und implementiert wird				
A.14.2.1	Leitlinie für sichere Entwicklung	Es müssen Regeln für die Entwicklung von Software und Systemen festgelegt und bei Entwicklungen innerhalb der Organisation angewandt werden.	ja	100%	Geschäftliche Anforderung
A.14.2.2	Änderungskontrollverfahren	Die Umsetzung von Änderungen muss einem formalen Änderungskontrollverfahren unterliegen.	ja	100%	Geschäftliche Anforderung
A.14.2.3	Technische Prüfung von Anwendunge nach Wechsel der Betriebsplattform	Bei einem Wechsel der Betriebsplattform müssen geschäftskritische Anwendungen geprüft und getestet werden, u sicherzustellen, dass keine negativen Auswirkungen auf die Betriebstätigkeit oder die Sicherheit der Organisation gibt.	ja	100%	Geschäftliche Anforderung
A.14.2.4	Beschränkungen von Änderungen an Software-Paketen	Von Änderungen an Software-Paketen ist abzuraten. Falls doch Änderungen vorgenommen werden, müssen diese auf das Notwendige beschränkt sein und in jedem Fall streng kontrollier werden.	ja	100%	Geschäftliche Anforderung
A.14.2.5	Systementwicklungsverfahren	Es sind Grundsätze für die Entwicklung sicherer Systeme festzulegen, zu dokumentieren, aufrechtzuerhalten und bei jede Systementwicklungsvorhaben anzuwenden.	ja	100%	Geschäftliche Anforderung
A.14.2.6	Sichere Entwicklungsumgebung	Organisation müssen eine sichere Entwicklungsumgebung für Systementwicklungen und Integrationsvorhaben, die den gesam Zyklus der Systementwicklung abdeckt, herstellen und angemessen schützen.	ja	100%	Geschäftliche Anforderung
A.14.2.7	Ausgelagerte Entwicklung	Die Organisation muss ausgelagerte Systementwicklungstätigkeiten beaufsichtigen und überwachen.	ja	100%	Geschäftliche Anforderung
A.14.2.8	Systemsicherheitsprüfungen	Während der Entwicklung müssen die Sicherheitsvorkehrungen auf Funktion geprüft werden.	ja	100%	Geschäftliche Anforderung

Nr.	Anforderung ISO 27001:2013	Beschreibung der Anforderung	Anwendbar	Status	Begründung der Nicht-/Anwendbarkeit
A.14.2.9	Systemabnahmeprüfung	Für neue Informationssysteme, Upgrades und neue Versionen sind Abnahmeprüfungsprogramme und dazugehörige Kriterien festzulegen.	ja	100%	Geschäftliche Anforderung
A.14.3	Prüfdaten Ziel: Sicherstellung des Schutzes von zu Prüfzwecken verwendeten Daten				
A.14.3.1	Schutz von Prüfdaten	Prüfdaten müssen sorgfältig ausgewählt, geschützt und kontrolli werden.	ja	100%	Geschäftliche Anforderung Gesetzliche Vorgabe
A.15	Lieferantenbeziehungen				
A.15.1	Sicherheit in Lieferantenbeziehungen Ziel: Sicherstellung des Schutzes der für Lieferanten zugänglichen Informationen des Unternehmens				
A.15.1.1	Informationssicherheitsleitlinie für Lieferantenbeziehungen	Die Informationssicherheitsanforderungen zur Verringerung von Risiken im Zusammenhang mit dem Zugriff von Lieferanten auf Informationen oder informationsverarbeitenden Einrichtungen de Organisation sind zu dokumentieren.	ja	100%	Geschäftliche Anforderung
A.15.1.2	Sicherheitsthemen in Lieferantenverträgen	Mit jedem Lieferanten, der u.U. Zugriff auf Informationen der Organisation hat, sie verarbeitet, speichert, weitergibt oder IT-Infrastrukturkomponenten dafür bereitstellt, müssen jeweils alle relevanten Informationssicherheitsanforderungen festgelegt und vereinbart werden.	ja	100%	Geschäftliche Anforderung Gesetzliche Vorgabe
A.15.1.3	IKT-Lieferkette	Vereinbarungen mit Lieferanten müssen Anforderungen für den Umgang mit Informationssicherheitsrisiken im Zusammenhang mit der Dienstleistungs- und Produktlieferkette im Bereich der Informations- und Kommunikationstechnologie enthalten.	ja	100%	Geschäftliche Anforderung Gesetzliche Vorgabe
A.15.2	Management der Dienstleistungserbringung durch Lieferanten Ziel: Aufrechterhaltung einer vereinbarten Informationssicherheitsstufe und Dienstleistungserbringung im Einklang mit Lieferantenverträgen				
A.15.2.1	Überwachung und Prüfung von Lieferantendienstleistungen	Organisationen müssen die Dienstleistungserbringung durch Lieferanten regelmäßig überwachen, prüfen und auditieren.	ja	100%	Geschäftliche Anforderung Gesetzliche Vorgabe
A.15.2.2	Management von Änderungen an Lieferantendienstleistungen	Änderungen an der Erbringung von Dienstleistungen durch Lieferanten einschließlich der Pflege und Verbesserung bestehender Informationssicherheitsleitlinien, -verfahren und -kontrollen müssen unter Berücksichtigung der Betriebswichtigke der betroffenen geschäftlichen Informationen, Systeme und Prozesse sowie einer erneuten Risikobewertung verwaltet werd	ja	100%	Geschäftliche Anforderung
A.16	Management von Informationssicherheitsvorfällen				
A.16.1	Management von Informationssicherheitsvorfällen und Verbesserungen Ziel: Sicherstellung einer konsistenten und wirksamen Strategie für das Management von Informationssicherheitsvorfällen einschließlich Benachrichtigung über Sicherheitsvorfälle und Schwachstellen				
A.16.1.1	Zuständigkeiten und Verfahren	Zuständigkeiten und Verfahren für das Management sind festzulegen, damit schnell, effektiv und koordiniert auf Informationssicherheitsvorfälle reagiert werden.	ja	100%	Geschäftliche Anforderung Gesetzliche Vorgabe
A.16.1.2	Meldung von Informationssicherheitsereignissen	Informationssicherheitsereignisse müssen so schnell wie möglic über geeignete Management-Kanäle gemeldet werden.	ja	100%	Geschäftliche Anforderung
A.16.1.3	Meldung von Informationssicherheits-Schwachstellen	Mitarbeiter und externe Parteien, die die Informationssysteme u -dienste der Organisation nutzen, müssen dazu aufgefordert werden, jegliche beobachteten oder vermuteten Informationssicherheitsschwachstellen in Systemen oder Diensten festzuhalten und zu melden.	ja	100%	Geschäftliche Anforderung
A.16.1.4	Bewertung und Einstufung von Informationssicherheitsereignissen	Informationssicherheitsereignisse sind zu bewerten, und es mus darüber entschieden werden, ob sie als Informationssicherheitsvorfälle eingestuft werden.	ja	100%	Geschäftliche Anforderung
A.16.1.5	Reaktion auf Informationssicherheitsvorfälle	Auf Informationssicherheitsvorfälle muss entsprechend den dokumentierten Verfahren reagiert werden.	ja	100%	Geschäftliche Anforderung Gesetzliche Vorgabe

Nr.	Anforderung ISO 27001:2013	Beschreibung der Anforderung	Anwendbar	Status	Begründung der Nicht-/Anwendbarkeit
A.16.1.6	Erkenntnisse aus Informationssicherheitsvorfällen	Aus der Analyse und Lösung von Informationssicherheitsvorfälle gewonnene Erkenntnisse müssen dazu genutzt werden, Auftretenswahrscheinlichkeit oder die Auswirkungen zukünftiger Vorfälle zu verringern.	ja	100%	Geschäftliche Anforderung
A.16.1.7	Sammeln von Beweismaterial	Die Organisation muss verfahren für die Ermittlung, Sammlung, Aneignung und Aufbewahrung von Informationen, die als Beweismaterial dienen können, festlegen und anwenden.	ja	100%	Geschäftliche Anforderung Gesetzliche Vorgabe
A.17	Informationssicherheitsaspekte des Business Continuity Management				
A.17.1	Kontinuität der Informationssicherheit Ziel: Die Kontinuität der Informationssicherheit muss Teil des Business Continuity Management (BCM) der Organisation sein, so dass sichergestellt ist, dass Informationen jederzeit geschützt sind und die Organisation auf negative Ereignisse vorbereitet ist.				
A.17.1.1	Planung der Kontinuität der Informationssicherheit	Die Organisation muss ihre Anforderungen für die Informationssicherheit und für die Aufrechterhaltung des Informationssicherheitsmanagements auch in schwierigen Situationen wie z.B. während einer Krise oder Katastrophe festlegen.	ja	100%	Geschäftliche Anforderung
A.17.1.2	Implementierung der Kontinuität der Informationssicherheit	Die Organisation muss Prozesse, Verfahren und Kontrollmaßnahmen festlegen, dokumentieren, implementieren und aufrechterhalten, um das erforderliche Maß an Kontinuität d Informationssicherheit in einer schwierigen Situation sicherstelle zu können.	ja	100%	Geschäftliche Anforderung Gesetzliche Vorgabe
A.17.1.3	Überprüfung, Überarbeitung und Auswertung der Kontinuität der Informationssicherheit	Die Organisation muss die festgelegten und implementierten Kontrollmaßnahmen für die Kontinuität der Informationssicherhe in regelmäßigen Abständen überprüfen, um sicherzustellen, das sie gültig und auch in schwierigen Situationen wirksam sind.	ja	100%	Geschäftliche Anforderung Gesetzliche Vorgabe
A.17.2	Redundanzen Ziel: Sicherstellung der Verfügbarkeit von informationsverarbeitenden Einrichtungen				
A.17.2.1	Verfügbarkeit von informationsverarbeitenden Einrichtungen	Informationsverarbeitende Einrichtungen müssen mit ausreichender Redundanz für die Einhaltung der Verfügbarkeitsanforderungen implementiert werden.	ja	100%	Geschäftliche Anforderung
A.18	Richtlinienkonformität				
A.18.1	Einhaltung gesetzlicher und vertraglicher Anforderungen Ziel: Vermeidung von Verstößen gegen gesetzliche, amtliche oder vertragliche Verpflichtungen im Zusammenhang mit Informationssicherheit sowie gegen jegliche Sicherheitsanforderungen				
A.18.1.1	Ermittlung anwendbarer gesetzlicher und vertraglicher Anforderungen	Alle relevanten gesetzlichen, amtlichen und vertraglichen Anforderungen sowie die Strategie der Organisation zur Erfüllun dieser Anforderungen müssen für jedes Informationssystem sow für die Organisation ausdrücklich ermittelt, dokumentiert und au dem neuesten Stand gehalten werden.	ja	100%	Geschäftliche Anforderung Gesetzliche Vorgabe
A.18.1.2	Rechte an geistigem Eigentum	Es sind angemessene Verfahren zu implementieren, mit denen Einhaltung gesetzlicher, amtlicher und vertraglicher Anforderungen zur Verwendung von Material, an dem möglicherweise Schutzrechte bestehen, sowie von urheberrechtlich geschützten Software-Produkten sichergestellt wird.	ja	100%	Geschäftliche Anforderung Gesetzliche Vorgabe
A.18.1.3	Schutz dokumentierter Informationen	Aufzeichnungen sind nach gesetzlichen, amtlichen, vertragliche und geschäftlichen Anforderungen vor Verlust, Zerstörung, Fälschung, unautorisiertem Zugriff und unautorisierter Freigabe schützen.	ja	100%	Geschäftliche Anforderung Gesetzliche Vorgabe
A.18.1.4	Privatsphäre und Schutz von personenbezogenen Informationen	Die Privatsphäre sowie der Schutz von personenbezogenen Informationen müssen entsprechend den Anforderungen der relevanten Gesetze, Vorschriften und ggf. Vertragsbestimmunge sichergestellt werden.	ja	100%	Geschäftliche Anforderung Gesetzliche Vorgabe
A.18.1.5	Regulierung kryptographischer Kontrollmaßnahmen	Kryptographische Kontrollmaßnahmen müssen unter Einhaltung aller relevanten Vereinbarungen, Gesetze und Vorschriften angewandt werden.	ja	100%	Geschäftliche Anforderung Gesetzliche Vorgabe

Nr.	Anforderung ISO 27001:2013	Beschreibung der Anforderung	Anwendbar	Status	Begründung der Nicht-/Anwendbarkeit
A.18.2	Informationssicherheitsprüfungen Ziel: Sicherstellung, dass Informationssicherheitsvorkehrungen entsprechend den Leitlinien und Verfahren der Organisation implementiert und angewandt wer				
A.18.2.1	Unabhängige Prüfung der Informationssicherheit	Die Strategie der Organisation für das Management der Informationssicherheit und deren Implementierung (d.h. Kontrollziele und -maßnahmen, Leitlinien, Prozesse und verfahr zur Informationssicherheit) müssen in planmäßigen Abständen oder jeweils bei erheblichen Änderungen an der Implementierun von Sicherheitsvorkehrungen durch eine unabhängige Stelle geprüft werden.	ja	100%	Geschäftliche Anforderung
A.18.2.2	Einhaltung der Sicherheitsleitlinien un -normen	Vorgesetzte müssen regelmäßig die Konformität der Informationsverarbeitung und der Verfahren in ihrem Zuständigkeitsbereich mit den jeweils anwendbaren Sicherheitslinien, Normen und jeglichen sonstigen Sicherheitsanforderungen prüfen.	ja	100%	Geschäftliche Anforderung
A.18.2.3	Inspektion der Technik auf Richtlinienkonformität	Informationssysteme müssen regelmäßig auf Konformität mit de Informationssicherheitsleitlinien und -normen der Organisation geprüft werden.	ja	100%	Geschäftliche Anforderung Gesetzliche Vorgabe