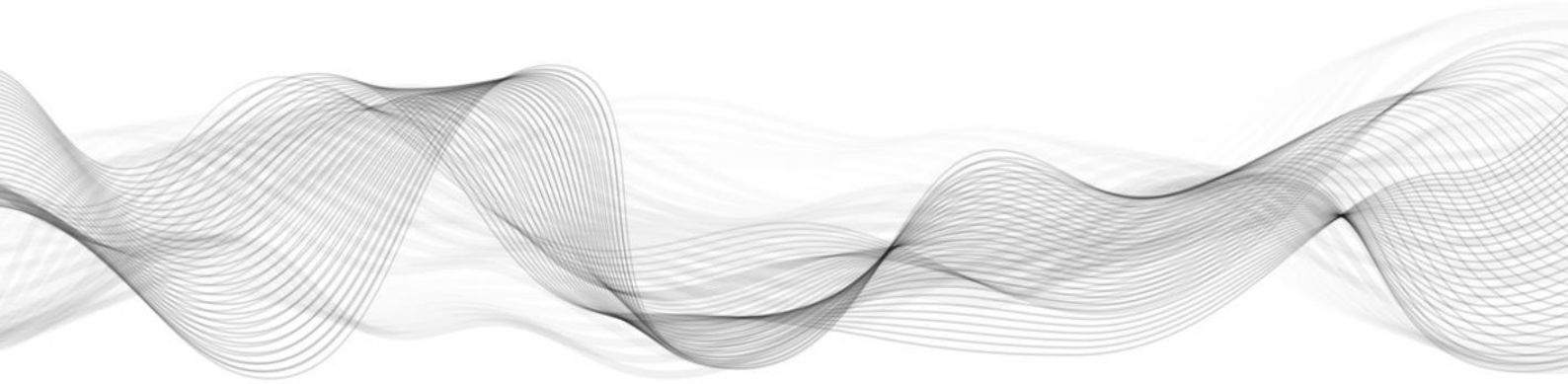
Statement of Applicability 2026



10.02.2026

Kapitel:
5 Organisationsbezogene Maßnahmen

Unterkapitel:
-

Maßnahmenziel:
Sicherstellung der kontinuierlichen Eignung, Angemessenheit, Wirksamkeit der Managementleitung und Unterstützung der Informationssicherheit in Übereinstimmung mit den Geschäftsanforderungen, gesetzlichen, gesetzlichen, regulatorischen und vertraglichen Anforderungen.

Maßnahmen:
5.01 Richtlinien für die Informationssicherheit

Massnahmentext:
Informationssicherheitsrichtlinien und themenspezifische Richtlinien sollten definiert, vom Management genehmigt, veröffentlicht, dem relevanten Personal und relevanten interessierten Parteien mitgeteilt und von ihnen bestätigt und in geplanten Abständen und bei wesentlichen Änderungen überprüft werden.

Anwendbarkeit:
Ja

Begründung:
-

Umsetzung:
https://alamos-support.atlassian.net/wiki/spaces/ISMS/embed/3551133700

Kapitel:
5 Organisationsbezogene Maßnahmen

Unterkapitel:
-

Maßnahmenziel:
Etablierung einer definierten, genehmigten und verstandenen Struktur für die Implementierung, den Betrieb und das Management der Informationssicherheit innerhalb der Organisation.

Maßnahmen:
5.02 Rollen und Verantwortlichkeiten in der Informationssicherheit

Massnahmentext:
Rollen und Verantwortlichkeiten für die Informationssicherheit sollten entsprechend den Anforderungen der Organisation definiert und zugewiesen werden.

Anwendbarkeit:
Ja

Begründung:
-

Umsetzung:

https://alamos-support.atlassian.net/wiki/x/E4Co0w

Kapitel:
5 Organisationsbezogene Maßnahmen

Unterkapitel:
-

Maßnahmenziel:
Reduzierung des Risikos von Betrug, Fehlern und Umgehung von Informationssicherheitskontrollen.

Maßnahmen:
5.03 Aufgabentrennung

Massnahmentext:
Widersprüchliche Aufgaben und Verantwortungsbereiche sollten getrennt werden.

Anwendbarkeit:
Ja

Begründung:
-

Umsetzung:
https://alamos-support.atlassian.net/wiki/x/CwCr0w

Kapitel:
5 Organisationsbezogene Maßnahmen

Unterkapitel:
-

Maßnahmenziel:
Um sicherzustellen, dass das Management seine Rolle in der Informationssicherheit versteht und Maßnahmen ergreift, die darauf abzielen, sicherzustellen, dass alle Mitarbeiter ihre Verantwortung für die Informationssicherheit kennen und erfüllen.

Maßnahmen:
5.04 Verantwortlichkeiten des Managements

Massnahmentext:
Das Management sollte von allen Mitarbeitern verlangen, dass sie die Informationssicherheit in Übereinstimmung mit der festgelegten Informationssicherheitsrichtlinie, den themenspezifischen Richtlinien und Verfahren der Organisation anwenden.

Anwendbarkeit:
Ja

Begründung:
-

Umsetzung:

https://alamos-support.atlassian.net/wiki/x/G4Co0w

Kapitel:
5 Organisationsbezogene Maßnahmen

Unterkapitel:
-

Maßnahmenziel:
Um einen angemessenen Informationsfluss in Bezug auf die Informationssicherheit zwischen der Organisation und den zuständigen Rechts-, Regulierungs- und Aufsichtsbehörden zu gewährleisten.

Maßnahmen:
5.05 Kontakt mit Behörden

Massnahmentext:
Die Organisation sollte Kontakte zu den zuständigen Behörden aufnehmen und pflegen.

Anwendbarkeit:
Ja

Begründung:
-

Umsetzung:
https://alamos-support.atlassian.net/wiki/x/GQCq0w

Kapitel:
5 Organisationsbezogene Maßnahmen

Unterkapitel:
-

Maßnahmenziel:
Sicherstellung eines angemessenen Informationsflusses in Bezug auf die Informationssicherheit.

Maßnahmen:
5.06 Kontakt zu speziellen Interessengruppen

Massnahmentext:
Die Organisation sollte Kontakte zu speziellen Interessengruppen oder anderen spezialisierten Sicherheitsforen und Berufsverbänden herstellen und pflegen.

Anwendbarkeit:
Ja

Begründung:
-

Umsetzung:
https://alamos-support.atlassian.net/wiki/x/DICp0w

Kapitel:
5 Organisationsbezogene Maßnahmen

Unterkapitel:
-

Maßnahmenziel:
Sensibilisierung für die Bedrohungsumgebung der Organisation, damit die entsprechenden Maßnahmen zur Schadensbegrenzung ergriffen werden können.

Maßnahmen:
5.07 Bedrohungsinformationen

Massnahmentext:
Informationen über Informationssicherheitsbedrohungen sollten gesammelt und analysiert werden, um Bedrohungsinformationen zu erstellen.

Anwendbarkeit:
Ja

Begründung:
-

Umsetzung:
https://alamos-support.atlassian.net/wiki/x/E4Cp0w

Kapitel:
5 Organisationsbezogene Maßnahmen

Unterkapitel:
-

Maßnahmenziel:
Sicherstellen, dass Informationssicherheitsrisiken im Zusammenhang mit Projekten und Ergebnissen im Projektmanagement während des gesamten Projektlebenszyklus effektiv angegangen werden.

Maßnahmen:
5.08 Informationssicherheit im Projektmanagement

Massnahmentext:
Sensibilisierung für die Bedrohungsumgebung der Organisation, damit die entsprechenden Maßnahmen zur Schadensbegrenzung ergriffen werden können.

Anwendbarkeit:
Ja

Begründung:
-

Umsetzung:
https://alamos-support.atlassian.net/wiki/x/GQCr0w

Kapitel:

5 Organisationsbezogene Maßnahmen

Unterkapitel:
-

Maßnahmenziel:
Um die Informationen der Organisation und andere damit verbundene Ressourcen zu identifizieren, um ihre Informationssicherheit zu gewährleisten und angemessene Eigentumsrechte zuzuweisen.

Maßnahmen:
5.09 Bestand an Informationen und anderen damit verbundenen Vermögenswerten

Massnahmentext:
Ein Inventar der Informationen und anderer damit verbundener Vermögenswerte, einschließlich der Eigentümer, sollte entwickelt und gepflegt werden.

Anwendbarkeit:
Ja

Begründung:
-

Umsetzung:
https://alamos-support.atlassian.net/wiki/x/GACl0w

Kapitel:
5 Organisationsbezogene Maßnahmen

Unterkapitel:
-

Maßnahmenziel:
Um sicherzustellen, dass Informationen und andere zugehörige Assets angemessen geschützt, verwendet und gehandhabt werden.

Maßnahmen:
5.10 Akzeptable Nutzung von Informationen und anderen damit verbundenen Vermögenswerten

Massnahmentext:
Regeln für die akzeptable Verwendung und Verfahren für den Umgang mit Informationen und anderen damit verbundenen Vermögenswerten sollten festgelegt, dokumentiert und umgesetzt werden.

Anwendbarkeit:
Ja

Begründung:
-

Umsetzung:
https://alamos-support.atlassian.net/wiki/x/FwCm0w

Kapitel:
5 Organisationsbezogene Maßnahmen

Unterkapitel:
-

Maßnahmenziel:
Um die Vermögenswerte der Organisation als Teil des Prozesses der Änderung oder Beendigung von Beschäftigung, Vertrag oder Vereinbarung zu schützen.

Maßnahmen:
5.11 Rückgabe von Werten

Massnahmentext:
Das Personal und gegebenenfalls andere interessierte Parteien sollten alle in ihrem Besitz befindlichen Vermögenswerte der Organisation bei Änderung oder Beendigung ihrer Beschäftigung, ihres Vertrags oder ihrer Vereinbarung zurückgeben.

Anwendbarkeit:
Ja

Begründung:
-

Umsetzung:
https://alamos-support.atlassian.net/wiki/x/KoCl0w

Kapitel:
5 Organisationsbezogene Maßnahmen

Unterkapitel:
-

Maßnahmenziel:
Sicherstellung der Identifizierung und des Verständnisses des Schutzbedarfs von Informationen in Übereinstimmung mit ihrer Bedeutung für die Organisation.

Maßnahmen:
5.12 Klassifizierung von Informationen

Massnahmentext:
Informationen sollten entsprechend den Informationssicherheitsanforderungen der Organisation auf der Grundlage von Vertraulichkeit, Integrität, Verfügbarkeit und relevanten Anforderungen interessierter Parteien klassifiziert werden.

Anwendbarkeit:
Ja

Begründung:
-

Umsetzung:
https://alamos-support.atlassian.net/wiki/x/LACq0w

Kapitel:
5 Organisationsbezogene Maßnahmen

Unterkapitel:
-

Maßnahmenziel:
Erleichterung der Kommunikation der Klassifizierung von Informationen und Unterstützung der Automatisierung der Informationsverarbeitung und -verwaltung.

Maßnahmen:
5.13 Kennzeichnung von Informationen

Massnahmentext:
Ein geeignetes Bündel von Verfahren für die Kennzeichnung von Informationen sollte in Übereinstimmung mit dem von der Organisation angenommenen Informationsklassifizierungsschema entwickelt und umgesetzt werden.

Anwendbarkeit:
Ja

Begründung:
-

Umsetzung:
https://alamos-support.atlassian.net/wiki/x/JACm0w

Kapitel:
5 Organisationsbezogene Maßnahmen

Unterkapitel:
-

Maßnahmenziel:
Um die Sicherheit von Informationen aufrechtzuerhalten, die innerhalb einer Organisation und mit jeder externen interessierten Partei übertragen werden.

Maßnahmen:
5.14 Informationstransfer

Massnahmentext:
Regeln, Verfahren oder Vereinbarungen für die Informationsübertragung sollten für alle Arten von Transfereinrichtungen innerhalb der Organisation und zwischen der Organisation und anderen Parteien vorhanden sein.

Anwendbarkeit:
Ja

Begründung:
-

Umsetzung:
https://alamos-support.atlassian.net/wiki/x/MwCq0w

Kapitel:
5 Organisationsbezogene Maßnahmen

Unterkapitel:
-

Maßnahmenziel:
Um den autorisierten Zugriff sicherzustellen und den unbefugten Zugriff auf Informationen und andere damit verbundene Ressourcen zu verhindern.

Maßnahmen:
5.15 Zugriffskontrolle

Massnahmentext:
Regeln zur Kontrolle des physischen und logischen Zugriffs auf Informationen und andere damit verbundene Ressourcen sollten auf der Grundlage der Geschäfts- und Informationssicherheitsanforderungen festgelegt und implementiert werden.

Anwendbarkeit:
Ja

Begründung:
-

Umsetzung:
https://alamos-support.atlassian.net/wiki/x/KACr0w

Kapitel:
5 Organisationsbezogene Maßnahmen

Unterkapitel:
-

Maßnahmenziel:
Um die eindeutige Identifizierung von Personen und Systemen zu ermöglichen, die auf die Informationen der Organisation und andere zugehörige Ressourcen zugreifen, und um eine angemessene Zuweisung von Zugriffsrechten zu ermöglichen.

Maßnahmen:
5.16 Identitätsmanagement

Massnahmentext:
Der gesamte Lebenszyklus von Identitäten sollte verwaltet werden.

Anwendbarkeit:
Ja

Begründung:
-

Umsetzung:
https://alamos-support.atlassian.net/wiki/x/OgCq0w

Kapitel:

5 Organisationsbezogene Maßnahmen

Unterkapitel:
-

Maßnahmenziel:
Um eine ordnungsgemäße Entitätsauthentifizierung sicherzustellen und Fehler von Authentifizierungsprozessen zu verhindern.

Maßnahmen:
5.17 Authentifizierungsinformationen

Massnahmentext:
Die Zuweisung und Verwaltung von Authentifizierungsinformationen sollte durch einen Verwaltungsprozess gesteuert werden, einschließlich der Beratung des Personals über den angemessenen Umgang mit Authentifizierungsinformationen.

Anwendbarkeit:
Ja

Begründung:
-

Umsetzung:
https://alamos-support.atlassian.net/wiki/x/GYCr0w

Kapitel:
5 Organisationsbezogene Maßnahmen

Unterkapitel:
-

Maßnahmenziel:
Um sicherzustellen, dass der Zugriff auf Informationen und andere damit verbundene Assets gemäß den Geschäftsanforderungen definiert und autorisiert wird.

Maßnahmen:
5.18 Zugriffsrechte

Massnahmentext:
Zugriffsrechte auf Informationen und andere zugehörige Ressourcen sollten in Übereinstimmung mit den themenspezifischen Richtlinien und Regeln der Organisation für die Zugriffskontrolle bereitgestellt, überprüft, geändert und entfernt werden.

Anwendbarkeit:
Ja

Begründung:
-

Umsetzung:
https://alamos-support.atlassian.net/wiki/x/PYCl0w

Kapitel:

5 Organisationsbezogene Maßnahmen

Unterkapitel:
-

Maßnahmenziel:
Aufrechterhaltung eines vereinbarten Niveaus der Informationssicherheit in Lieferantenbeziehungen.

Maßnahmen:
5.19 Informationssicherheit in Lieferantenbeziehungen

Massnahmentext:
Prozesse und Verfahren sollten definiert und implementiert werden, um die Informationssicherheitsrisiken zu bewältigen, die mit der Verwendung von Produkten oder Dienstleistungen des Lieferanten verbunden sind.

Anwendbarkeit:
Ja

Begründung:
-

Umsetzung:
https://alamos-support.atlassian.net/wiki/x/RICl0w

Kapitel:
5 Organisationsbezogene Maßnahmen

Unterkapitel:
-

Maßnahmenziel:
Aufrechterhaltung eines vereinbarten Niveaus der Informationssicherheit in Lieferantenbeziehungen.

Maßnahmen:
5.20 Berücksichtigung der Informationssicherheit im Rahmen von Lieferantenvereinbarungen

Massnahmentext:
Relevante Anforderungen an die Informationssicherheit sollten auf der Grundlage der Art der Lieferantenbeziehung festgelegt und mit jedem Lieferanten vereinbart werden.

Anwendbarkeit:
Ja

Begründung:
-

Umsetzung:
https://alamos-support.atlassian.net/wiki/x/RICl0w

Kapitel:

5 Organisationsbezogene Maßnahmen

Unterkapitel:
-

Maßnahmenziel:
Aufrechterhaltung eines vereinbarten Niveaus der Informationssicherheit in Lieferantenbeziehungen.

Maßnahmen:
5.21 Management der Informationssicherheit in der IKT-Lieferkette

Massnahmentext:
Prozesse und Verfahren sollten definiert und implementiert werden, um informationssicherheitsrisiken im Zusammenhang mit der Lieferkette für IKT-Produkte und -Dienstleistungen zu bewältigen.

Anwendbarkeit:
Ja

Begründung:
-

Umsetzung:
https://alamos-support.atlassian.net/wiki/x/RICl0w

Kapitel:
5 Organisationsbezogene Maßnahmen

Unterkapitel:
-

Maßnahmenziel:
Aufrechterhaltung eines vereinbarten Niveaus der Informationssicherheit und Der Erbringung von Dienstleistungen in Übereinstimmung mit den Lieferantenvereinbarungen.

Maßnahmen:
5.22 Überwachung, Überprüfung und Änderungsmanagement von Lieferantendienstleistungen

Massnahmentext:
Die Organisation sollte regelmäßig Änderungen in den Sicherheitspraktiken für Lieferanteninformationen und der Servicebereitstellung überwachen, überprüfen, bewerten und verwalten.

Anwendbarkeit:
Ja

Begründung:
-

Umsetzung:
https://alamos-support.atlassian.net/wiki/x/RICl0w

Kapitel:
5 Organisationsbezogene Maßnahmen

Unterkapitel:
-

Maßnahmenziel:
Zum Spezifizieren und Verwalten der Informationssicherheit für die Verwendung von Clouddiensten.

Maßnahmen:
5.23 Informationssicherheit für die Nutzung von Cloud-Diensten

Massnahmentext:
Prozesse für den Erwerb, die Nutzung, das Management und den Ausstieg aus Cloud-Diensten sollten in Übereinstimmung mit den Informationssicherheitsanforderungen des Unternehmens eingerichtet werden.

Anwendbarkeit:
Ja

Begründung:
-

Umsetzung:
https://alamos-support.atlassian.net/wiki/x/GICC3Q

Kapitel:
5 Organisationsbezogene Maßnahmen

Unterkapitel:
-

Maßnahmenziel:
Gewährleistung einer schnellen, effektiven, konsistenten und geordneten Reaktion auf Informationssicherheitsvorfälle, einschließlich der Kommunikation über Informationssicherheitsereignisse.

Maßnahmen:
5.24 Planung und Vorbereitung des Managements von Informationssicherheitsvorfällen

Massnahmentext:
Die Organisation sollte die Verwaltung von Informationssicherheitsvorfällen planen und vorbereiten, indem sie Prozesse, Rollen und Verantwortlichkeiten für das Management von Informationssicherheitsvorfällen definiert, einrichtet und kommuniziert.

Anwendbarkeit:
Ja

Begründung:
-

Umsetzung:
https://alamos-support.atlassian.net/wiki/x/J4Cr0w

Kapitel:
5 Organisationsbezogene Maßnahmen

Unterkapitel:
-

Maßnahmenziel:
Um eine effektive Kategorisierung und Priorisierung von Informationssicherheitsereignissen sicherzustellen.

Maßnahmen:
5.25 Bewertung und Entscheidung über Informationssicherheitsereignisse

Massnahmentext:
Die Organisation sollte Informationssicherheitsereignisse bewerten und entscheiden, ob sie als Informationssicherheitsvorfälle kategorisiert werden sollen.

Anwendbarkeit:
Ja

Begründung:
-

Umsetzung:
https://alamos-support.atlassian.net/wiki/x/SQCq0w

Kapitel:
5 Organisationsbezogene Maßnahmen

Unterkapitel:
-

Maßnahmenziel:
Um eine effiziente und effektive Reaktion auf Informationssicherheitsvorfälle zu gewährleisten.

Maßnahmen:
5.26 Reaktion auf Informationssicherheitsvorfälle

Massnahmentext:
Auf Informationssicherheitsvorfälle sollte gemäß den dokumentierten Verfahren reagiert werden.

Anwendbarkeit:
Ja

Begründung:
-

Umsetzung:
https://alamos-support.atlassian.net/wiki/x/JoCp0w

Kapitel:
5 Organisationsbezogene Maßnahmen

Unterkapitel:
-

Maßnahmenziel:
Um die Wahrscheinlichkeit oder die Folgen zukünftiger Vorfälle zu reduzieren.

Maßnahmen:
5.27 Aus Informationssicherheitsvorfällen lernen

Massnahmentext:
Die aus Informationssicherheitsvorfällen gewonnenen Erkenntnisse sollten genutzt werden, um die Informationssicherheitskontrollen zu stärken und zu verbessern.

Anwendbarkeit:
Ja

Begründung:
-

Umsetzung:
https://alamos-support.atlassian.net/wiki/x/KwCl0w

Kapitel:
5 Organisationsbezogene Maßnahmen

Unterkapitel:
-

Maßnahmenziel:
Gewährleistung einer konsistenten und effektiven Verwaltung von Beweismitteln im Zusammenhang mit Informationssicherheitsvorfällen zum Zwecke disziplinarischer und rechtlicher Maßnahmen.

Maßnahmen:
5.28 Sammlung von Beweismitteln

Massnahmentext:
Die Organisation sollte Verfahren zur Identifizierung, Sammlung, Erfassung und Sicherung von Beweismitteln im Zusammenhang mit Informationssicherheitsereignissen festlegen und umsetzen.

Anwendbarkeit:
Ja

Begründung:
-

Umsetzung:
https://alamos-support.atlassian.net/wiki/x/S4Cl0w

Kapitel:
5 Organisationsbezogene Maßnahmen

Unterkapitel:

-

Maßnahmenziel:
Zum Schutz von Informationen und anderen zugehörigen Ressourcen bei Störungen.

Maßnahmen:
5.29 Informationssicherheit bei Störungen

Massnahmentext:
Die Organisation sollte planen, wie die Informationssicherheit während einer Unterbrechung auf einem angemessenen Niveau gehalten werden kann.

Anwendbarkeit:
Ja

Begründung:
-

Umsetzung:
https://alamos-support.atlassian.net/wiki/x/QYCo0w

Kapitel:
5 Organisationsbezogene Maßnahmen

Unterkapitel:
-

Maßnahmenziel:
Um die Verfügbarkeit der Informationen der Organisation und anderer damit verbundener Ressourcen während Störungen sicherzustellen.

Maßnahmen:
5.30 IKT-Bereitschaft für Business Continuity

Massnahmentext:
Die IKT-Bereitschaft sollte auf der Grundlage der Geschäftskontinuitätsziele und der Anforderungen an die IKT-Kontinuität geplant, implementiert, aufrechterhalten und getestet werden.

Anwendbarkeit:
Ja

Begründung:
-

Umsetzung:
https://alamos-support.atlassian.net/wiki/x/NACm0w

Kapitel:
5 Organisationsbezogene Maßnahmen

Unterkapitel:
-

Maßnahmenziel:
Um die Einhaltung gesetzlicher, gesetzlicher, regulatorischer und vertraglicher Anforderungen im Zusammenhang mit der Informationssicherheit sicherzustellen.

Maßnahmen:
5.31 Gesetzliche, gesetzliche, regulatorische und vertragliche Anforderungen

Massnahmentext:
Gesetzliche, gesetzliche, regulatorische und vertragliche Anforderungen, die für die Informationssicherheit relevant sind, und der Ansatz der Organisation zur Erfüllung dieser Anforderungen sollten identifiziert, dokumentiert und auf dem neuesten Stand gehalten werden.

Anwendbarkeit:
Ja

Begründung:
-

Umsetzung:
https://alamos-support.atlassian.net/wiki/x/M4Cp0w

Kapitel:
5 Organisationsbezogene Maßnahmen

Unterkapitel:
-

Maßnahmenziel:
Um die Einhaltung gesetzlicher, gesetzlicher, regulatorischer und vertraglicher Anforderungen in Bezug auf geistige Eigentumsrechte und die Verwendung proprietärer Produkte sicherzustellen.

Maßnahmen:
5.32 Rechte an geistigem Eigentum

Massnahmentext:
Die Organisation sollte geeignete Verfahren zum Schutz der Rechte an geistigem Eigentum einführen.

Anwendbarkeit:
Ja

Begründung:
-

Umsetzung:
https://alamos-support.atlassian.net/wiki/x/WICl0w

Kapitel:
5 Organisationsbezogene Maßnahmen

Unterkapitel:
-

Maßnahmenziel:
Um die Einhaltung gesetzlicher, gesetzlicher, regulatorischer und vertraglicher Anforderungen sowie der Erwartungen der Gemeinschaft oder der Gesellschaft in Bezug auf den Schutz und die Verfügbarkeit von Aufzeichnungen sicherzustellen.

Maßnahmen:
5.33 Schutz von Aufzeichnungen

Massnahmentext:
Aufzeichnungen sollten vor Verlust, Zerstörung, Verfälschung, unbefugtem Zugriff und unbefugter Freigabe geschützt werden.

Anwendbarkeit:
Ja

Begründung:
-

Umsetzung:
https://alamos-support.atlassian.net/wiki/x/OwCm0w

Kapitel:
5 Organisationsbezogene Maßnahmen

Unterkapitel:
-

Maßnahmenziel:
Sicherstellung der Einhaltung gesetzlicher, gesetzlicher, regulatorischer und vertraglicher Anforderungen in Bezug auf die Informationssicherheitsaspekte des pbD-Schutzes.

Maßnahmen:
5.34 Privatsphäre und Schutz von pbD

Massnahmentext:
Die Organisation sollte die Anforderungen an die Wahrung der Privatsphäre und den Schutz von pbD gemäß den geltenden Gesetzen und Vorschriften sowie den vertraglichen Anforderungen identifizieren und erfüllen.

Anwendbarkeit:
Ja

Begründung:
-

Umsetzung:
https://alamos-support.atlassian.net/wiki/x/MgCl0w

Kapitel:
5 Organisationsbezogene Maßnahmen

Unterkapitel:
-

Maßnahmenziel:
Um die kontinuierliche Eignung, Angemessenheit und Wirksamkeit des Ansatzes der Organisation für das Management der Informationssicherheit sicherzustellen.

Maßnahmen:
5.35 Unabhängige Überprüfung der Informationssicherheit

Massnahmentext:
Der Ansatz der Organisation für das Management der Informationssicherheit und deren Implementierung, einschließlich Personen, Prozessen und Technologien, sollte in geplanten Intervallen oder bei wesentlichen Änderungen unabhängig überprüft werden.

Anwendbarkeit:
Ja

Begründung:
-

Umsetzung:
https://alamos-support.atlassian.net/wiki/x/OoCp0w

Kapitel:
5 Organisationsbezogene Maßnahmen

Unterkapitel:
-

Maßnahmenziel:
Um sicherzustellen, dass die Informationssicherheit in Übereinstimmung mit den Informationssicherheitsrichtlinien der Organisation, den themenspezifischen Richtlinien, Regeln und Standards implementiert und betrieben wird.

Maßnahmen:
5.36 Konformität mit Richtlinien, Regeln und Standards für Informationssicherheit

Massnahmentext:
Die Einhaltung der Informationssicherheitsrichtlinie des Unternehmens, der themenspezifischen Richtlinien, Regeln und Standards sollte regelmäßig überprüft werden.

Anwendbarkeit:
Ja

Begründung:
-

Umsetzung:
https://alamos-support.atlassian.net/wiki/x/TYAa3g

Kapitel:
5 Organisationsbezogene Maßnahmen

Unterkapitel:
-

Maßnahmenziel:
Um den korrekten und sicheren Betrieb von Informationsverarbeitungsanlagen zu gewährleisten.

Maßnahmen:
5.37 Dokumentierte Betriebsabläufe

Massnahmentext:
Die Betriebsverfahren für Informationsverarbeitungsanlagen sollten dokumentiert und dem Personal zur Verfügung gestellt werden, das sie benötigt.

Anwendbarkeit:
Ja

Begründung:
-

Umsetzung:
https://alamos-support.atlassian.net/wiki/x/LwCr0w

Kapitel:
6 Personenbezogene Maßnahmen

Unterkapitel:
-

Maßnahmenziel:
Um sicherzustellen, dass alle Mitarbeiter für die Rollen, für die sie in Betracht gezogen werden, geeignet und geeignet sind und während ihrer Beschäftigung berechtigt und geeignet bleiben.

Maßnahmen:
6.01 Durchleuchtung (personell)

Massnahmentext:
Hintergrundüberprüfungen aller Kandidaten, die Personal werden sollen, sollten vor dem Eintritt in die Organisation und unter Berücksichtigung der geltenden Gesetze, Vorschriften und Ethiken kontinuierlich durchgeführt werden und proportional zu den Geschäftsanforderungen, der Klassifizierung der zu handhabenden Informationen und den wahrgenommenen Risiken sein.

Anwendbarkeit:
Ja

Begründung:
-

Umsetzung:
https://alamos-support.atlassian.net/wiki/x/hYCr0w

Kapitel:
6 Personenbezogene Maßnahmen

Unterkapitel:

-

Maßnahmenziel:
Um sicherzustellen, dass das Personal seine Verantwortlichkeiten für die Informationssicherheit für die Rollen versteht, für die es in Betracht gezogen wird.

Maßnahmen:
6.02 Arbeits- und Beschäftigungsbedingungen

Massnahmentext:
In den Arbeitsverträgen sollten die Verantwortlichkeiten des Personals und der Organisation für die Informationssicherheit festgelegt sein.

Anwendbarkeit:
Ja

Begründung:
-

Umsetzung:
https://alamos-support.atlassian.net/wiki/x/ooCl0w

Kapitel:
6 Personenbezogene Maßnahmen

Unterkapitel:
-

Maßnahmenziel:
Um sicherzustellen, dass das Personal und die relevanten interessierten Parteien sich ihrer Verantwortung für die Informationssicherheit bewusst sind und diese erfüllen.

Maßnahmen:
6.03 Informationssicherheitsbewusstsein, Aus- und Weiterbildung

Massnahmentext:
Das Personal der Organisation und relevante interessierte Parteien sollten ein angemessenes Informationssicherheitsbewusstsein, Aus- und Weiterbildung sowie regelmäßige Aktualisierungen der Informationssicherheitspolitik der Organisation, themenspezifischer Richtlinien und Verfahren erhalten, die für ihre berufliche Funktion relevant sind.

Anwendbarkeit:
Ja

Begründung:
-

Umsetzung:
https://alamos-support.atlassian.net/wiki/x/oQCq0w

Kapitel:
6 Personenbezogene Maßnahmen

Unterkapitel:
-

Maßnahmenziel:
Um sicherzustellen, dass das Personal und andere relevante interessierte Parteien die Folgen eines Verstoßes gegen die Informationssicherheitspolitik verstehen, um Personal, das den Verstoß begangen hat, abzuschrecken und angemessen damit umzugehen.

Maßnahmen:
6.04 Disziplinarverfahren

Massnahmentext:
Ein Disziplinarverfahren sollte formalisiert und kommuniziert werden, um Maßnahmen gegen Personal und andere relevante interessierte Parteien zu ergreifen, die einen Verstoß gegen die Informationssicherheitsrichtlinie begangen haben.

Anwendbarkeit:
Ja

Begründung:
-

Umsetzung:
https://alamos-support.atlassian.net/wiki/x/nQCl0w

Kapitel:
6 Personenbezogene Maßnahmen

Unterkapitel:
-

Maßnahmenziel:
Um die Interessen der Organisation als Teil des Prozesses der Änderung oder Beendigung von Arbeits- oder Verträgen zu schützen.

Maßnahmen:
6.05 Verantwortlichkeiten nach Beendigung oder Änderung des Arbeitsverhältnisses

Massnahmentext:
Verantwortlichkeiten und Pflichten im Bereich der Informationssicherheit, die nach Beendigung oder Änderung des Beschäftigungsverhältnisses gültig bleiben, sollten definiert, durchgesetzt und dem zuständigen Personal und anderen interessierten Parteien mitgeteilt werden.

Anwendbarkeit:
Ja

Begründung:
-

Umsetzung:
https://alamos-support.atlassian.net/wiki/x/awCm0w

Kapitel:
6 Personenbezogene Maßnahmen

Unterkapitel:
-

Maßnahmenziel:
Wahrung der Vertraulichkeit von Informationen, die für Mitarbeiter oder externe Parteien zugänglich sind.

Maßnahmen:
6.06 Vertraulichkeits- oder Geheimhaltungsvereinbarungen

Massnahmentext:
Vertraulichkeits- oder Geheimhaltungsvereinbarungen, die die Bedürfnisse der Organisation nach dem Schutz von Informationen widerspiegeln, sollten identifiziert, dokumentiert, regelmäßig überprüft und von Mitarbeitern und anderen relevanten interessierten Parteien unterzeichnet werden.

Anwendbarkeit:
Ja

Begründung:
-

Umsetzung:
https://alamos-support.atlassian.net/wiki/x/qYCl0w

Kapitel:
6 Personenbezogene Maßnahmen

Unterkapitel:
-

Maßnahmenziel:
Um die Sicherheit von Informationen zu gewährleisten, wenn das Personal aus der Ferne arbeitet.

Maßnahmen:
6.07 Remote-Arbeit

Massnahmentext:
Sicherheitsmaßnahmen sollten implementiert werden, wenn Mitarbeiter aus der Ferne arbeiten, um Informationen zu schützen, auf die außerhalb der Räumlichkeiten der Organisation zugegriffen, diese verarbeitet oder gespeichert werden.

Anwendbarkeit:
Ja

Begründung:
-

Umsetzung:
https://alamos-support.atlassian.net/wiki/x/AQAx0w

Kapitel:
6 Personenbezogene Maßnahmen

Unterkapitel:
-

Maßnahmenziel:
Unterstützung der zeitnahen, konsistenten und effektiven Berichterstattung über Informationssicherheitsereignisse, die vom Personal identifiziert werden können.

Maßnahmen:
6.08 Berichte zu Informationssicherheitsereignissen

Massnahmentext:
Die Organisation sollte einen Mechanismus für das Personal bereitstellen, um beobachtete oder vermutete Informationssicherheitsereignisse über geeignete Kanäle rechtzeitig zu melden.

Anwendbarkeit:
Ja

Begründung:
-

Umsetzung:
https://alamos-support.atlassian.net/wiki/x/swCl0w

Kapitel:
7 Physiche Maßnahmen

Unterkapitel:
-

Maßnahmenziel:
Um unbefugten physischen Zugriff, Beschädigung und Eingriff in die Informationen der Organisation und andere damit verbundene Vermögenswerte zu verhindern.

Maßnahmen:
7.01 Physische Sicherheitsperimeter

Massnahmentext:
Sicherheitsperimeter sollten definiert und verwendet werden, um Bereiche zu schützen, die Informationen und andere zugehörige Ressourcen enthalten.

Anwendbarkeit:
Ja

Begründung:
-

Umsetzung:
https://alamos-support.atlassian.net/wiki/x/ugCl0w

Kapitel:

7 Physiche Maßnahmen

Unterkapitel:
-

Maßnahmenziel:
Um sicherzustellen, dass nur autorisierter physischer Zugriff auf die Informationen der Organisation und andere zugehörige Ressourcen erfolgt.

Maßnahmen:
7.02 Physischer Eintritt (Zutrittskontrolle)

Massnahmentext:
Sichere Bereiche sollten durch geeignete Zugangskontrollen und Zugangspunkte geschützt werden.

Anwendbarkeit:
Ja

Begründung:
-

Umsetzung:
https://alamos-support.atlassian.net/wiki/x/doCq0w

Kapitel:
7 Physiche Maßnahmen

Unterkapitel:
-

Maßnahmenziel:
Um unbefugten physischen Zugriff, Schäden und Eingriffe in die Informationen der Organisation und andere damit verbundene Vermögenswerte in Büros, Räumen und Einrichtungen zu verhindern.

Maßnahmen:
7.03 Sicherung von Büros, Räumen und Einrichtungen

Massnahmentext:
Physische Sicherheit für Büros, Räume und Einrichtungen sollte entworfen und umgesetzt werden.

Anwendbarkeit:
Ja

Begründung:
-

Umsetzung:
https://alamos-support.atlassian.net/wiki/x/sICl0w

Kapitel:
7 Physiche Maßnahmen

Unterkapitel:
-

Maßnahmenziel:
Um unbefugten physischen Zugriff zu erkennen und abzuschrecken.

Maßnahmen:
7.04 Physische Sicherheitsüberwachung

Massnahmentext:
Räumlichkeiten sollten kontinuierlich auf unbefugten physischen Zugriff überwacht werden.

Anwendbarkeit:
Ja

Begründung:
-

Umsetzung:
https://alamos-support.atlassian.net/wiki/x/fYCq0w

Kapitel:
7 Physiche Maßnahmen

Unterkapitel:
-

Maßnahmenziel:
Um die Folgen von Ereignissen, die von physischen und Umweltbedrohungen ausgehen, zu verhindern oder zu reduzieren.

Maßnahmen:
7.05 Schutz vor physischen und Umweltbedrohungen

Massnahmentext:
Der Schutz vor physischen und Umweltbedrohungen wie Naturkatastrophen und anderen vorsätzlichen oder unbeabsichtigten physischen Bedrohungen der Infrastruktur sollte konzipiert und umgesetzt werden.

Anwendbarkeit:
Ja

Begründung:
-

Umsetzung:
https://alamos-support.atlassian.net/wiki/x/fgCm0w

Kapitel:
7 Physiche Maßnahmen

Unterkapitel:
-

Maßnahmenziel:
Um Informationen und andere damit verbundene Vermögenswerte in sicheren Bereichen vor Schäden und unbefugten Eingriffen durch das in diesen Bereichen tätige Personal zu schützen.

Maßnahmen:
7.06 Arbeiten in sicheren Bereichen

Massnahmentext:
Sicherheitsmaßnahmen für die Arbeit in sicheren Bereichen sollten konzipiert und umgesetzt werden.

Anwendbarkeit:
Ja

Begründung:
-

Umsetzung:
https://alamos-support.atlassian.net/wiki/x/iYCq0w

Kapitel:
7 Physiche Maßnahmen

Unterkapitel:
-

Maßnahmenziel:
Verringerung des Risikos von unbefugtem Zugriff, Verlust und Beschädigung von Informationen auf Schreibtischen, Bildschirmen und an anderen zugänglichen Orten während und außerhalb der normalen Arbeitszeiten.

Maßnahmen:
7.07 Aufgeräumter Schreibtisch und Bildschirm

Massnahmentext:
Klare Schreibtischregeln für Papiere und Wechselmedien sowie klare Bildschirmregeln für Informationsverarbeitungseinrichtungen sollten definiert und angemessen durchgesetzt werden.

Anwendbarkeit:
Ja

Begründung:
-

Umsetzung:
https://alamos-support.atlassian.net/wiki/x/AYAz0w

Kapitel:
7 Physiche Maßnahmen

Unterkapitel:
-

Maßnahmenziel:
Reduzierung der Risiken durch physische und Umweltbedrohungen sowie durch unbefugten Zugriff und Beschädigung.

Maßnahmen:
7.08 Standortwahl und Schutz der Geräte

Massnahmentext:
Die Ausrüstung sollte sicher und geschützt aufgestellt werden.

Anwendbarkeit:
Ja

Begründung:
-

Umsetzung:
https://alamos-support.atlassian.net/wiki/x/A4Cs0w

Kapitel:
7 Physiche Maßnahmen

Unterkapitel:
-

Maßnahmenziel:
Um Verlust, Beschädigung, Diebstahl oder Kompromittierung von externen Assets und Unterbrechungen des Betriebs der Organisation zu verhindern.

Maßnahmen:
7.09 Sicherheit von Vermögenswerten außerhalb von Räumlichkeiten

Massnahmentext:
Externe Assets sollten geschützt werden.

Anwendbarkeit:
Ja

Begründung:
-

Umsetzung:
https://alamos-support.atlassian.net/wiki/x/yACq0w

Kapitel:
7 Physiche Maßnahmen

Unterkapitel:
-

Maßnahmenziel:
Nur autorisierte Offenlegung, Änderung, Entfernung oder Zerstörung von Informationen auf Speichermedien zu gewährleisten.

Maßnahmen:
7.10 Speichermedien

Massnahmentext:
Speichermedien sollten während ihres gesamten Lebenszyklus von Beschaffung, Verwendung, Transport und Entsorgung in Übereinstimmung mit dem Klassifizierungsschema und den Handhabungsanforderungen der Organisation verwaltet werden.

Anwendbarkeit:
Ja

Begründung:
-

Umsetzung:
https://alamos-support.atlassian.net/wiki/x/xgCr0w

Kapitel:
7 Physiche Maßnahmen

Unterkapitel:
-

Maßnahmenziel:
Um den Verlust, die Beschädigung oder die Kompromittierung von Informationen und anderen damit verbundenen Ressourcen oder eine Unterbrechung des Betriebs der Organisation aufgrund des Ausfalls und der Unterbrechung der unterstützenden Versorgungsunternehmen zu verhindern.

Maßnahmen:
7.11 Versorgungseinrichtungen

Massnahmentext:
Informationsverarbeitungsanlagen sollten vor Stromausfällen und anderen Störungen geschützt werden, die durch Ausfälle in unterstützenden Versorgungseinrichtungen verursacht werden.

Anwendbarkeit:
Ja

Begründung:
-

Umsetzung:
https://alamos-support.atlassian.net/wiki/x/pYCr0w

Kapitel:
7 Physiche Maßnahmen

Unterkapitel:
-

Maßnahmenziel:

Um Verlust, Beschädigung, Diebstahl oder Kompromittierung von Informationen und anderen damit verbundenen Vermögenswerten sowie Unterbrechungen des Betriebs der Organisation im Zusammenhang mit der Strom- und Kommunikationsverkabelung zu verhindern.

Maßnahmen:
7.12 Sicherheit der Verkabelung

Massnahmentext:
Kabel, die Strom, Daten oder unterstützende Informationsdienste befördern, sollten vor Abfangen, Störungen oder Beschädigungen geschützt werden.

Anwendbarkeit:
Ja

Begründung:
-

Umsetzung:
https://alamos-support.atlassian.net/wiki/x/6ACr0w

Kapitel:
7 Physiche Maßnahmen

Unterkapitel:
-

Maßnahmenziel:
Um Verlust, Beschädigung, Diebstahl oder Kompromittierung von Informationen und anderen damit verbundenen Vermögenswerten sowie Unterbrechungen des Betriebs der Organisation aufgrund mangelnder Wartung zu verhindern.

Maßnahmen:
7.13 Instandhaltung von Geräten und Betriebsmitteln

Massnahmentext:
Die Ausrüstung sollte ordnungsgemäß gewartet werden, um die Verfügbarkeit, Integrität und Vertraulichkeit der Informationen zu gewährleisten.

Anwendbarkeit:
Ja

Begründung:
-

Umsetzung:
https://alamos-support.atlassian.net/wiki/x/zICo0w

Kapitel:
7 Physiche Maßnahmen

Unterkapitel:
-

Maßnahmenziel:
Um das Durchsickern von Informationen von Geräten zu verhindern, die entsorgt oder wiederverwendet werden sollen.

Maßnahmen:
7.14 Sichere Entsorgung oder Wiederverwendung von Geräten und Betriebsmitteln

Massnahmentext:
Geräte, die Speichermedien enthalten, sollten überprüft werden, um sicherzustellen, dass sensible Daten und lizenzierte Software vor der Entsorgung oder Wiederverwendung entfernt oder sicher überschrieben wurden.

Anwendbarkeit:
Ja

Begründung:
-

Umsetzung:
https://alamos-support.atlassian.net/wiki/x/7wCr0w

Kapitel:
8 Technische Maßnahmen

Unterkapitel:
-

Maßnahmenziel:
Zum Schutz von Informationen vor den Risiken, die durch die Verwendung von Benutzerendgeräten entstehen.

Maßnahmen:
8.01 Benutzer-Endgeräte

Massnahmentext:
Informationen, die auf Benutzerendgeräten gespeichert, von diesen verarbeitet werden oder über Benutzerendgeräte zugänglich sind, sollten geschützt werden.

Anwendbarkeit:
Ja

Begründung:
-

Umsetzung:
https://alamos-support.atlassian.net/wiki/x/BQCs0w

Kapitel:
8 Technische Maßnahmen

Unterkapitel:
-

Maßnahmenziel:

Um sicherzustellen, dass nur autorisierte Benutzer, Softwarekomponenten und Dienste mit privilegierten Zugriffsrechten versehen werden.

Maßnahmen:
8.02 Privilegierte Zugriffsrechte

Massnahmentext:
Die Vergabe und Nutzung privilegierter Zugriffsrechte sollte eingeschränkt und verwaltet werden.

Anwendbarkeit:
Ja

Begründung:
-

Umsetzung:
https://alamos-support.atlassian.net/wiki/x/G4Cs0w

Kapitel:
8 Technische Maßnahmen

Unterkapitel:
-

Maßnahmenziel:
Um nur autorisierten Zugriff zu gewährleisten und unbefugten Zugriff auf Informationen und andere damit verbundene Assets zu verhindern.

Maßnahmen:
8.03 Informationszugangsbeschränkung

Massnahmentext:
Der Zugang zu Informationen und anderen damit verbundenen Ressourcen sollte im Einklang mit der festgelegten themenspezifischen Richtlinie zur Zugriffskontrolle eingeschränkt werden.

Anwendbarkeit:
Ja

Begründung:
-

Umsetzung:
https://alamos-support.atlassian.net/wiki/x/5YCo0w

Kapitel:
8 Technische Maßnahmen

Unterkapitel:
-

Maßnahmenziel:
Um die Einführung nicht autorisierter Funktionen zu verhindern, unbeabsichtigte oder

böswillige Änderungen zu vermeiden und die Vertraulichkeit wertvollen geistigen Eigentums zu wahren.

Maßnahmen:
8.04 Zugriff auf den Quellcode

Massnahmentext:
Lese- und Schreibzugriffe auf Quellcode, Entwicklungstools und Softwarebibliotheken sollten entsprechend verwaltet werden.

Anwendbarkeit:
Ja

Begründung:
-

Umsetzung:
https://alamos-support.atlassian.net/wiki/x/9wCl0w

Kapitel:
8 Technische Maßnahmen

Unterkapitel:
-

Maßnahmenziel:
Um sicherzustellen, dass ein Benutzer oder eine Entität sicher authentifiziert wird, wenn Zugriff auf Systeme, Anwendungen und Dienste gewährt wird.

Maßnahmen:
8.05 Sichere Authentifizierung

Massnahmentext:
Sichere Authentifizierungstechnologien und -verfahren sollten auf der Grundlage von Informationszugriffsbeschränkungen und der themenspezifischen Richtlinie zur Zugriffskontrolle implementiert werden.

Anwendbarkeit:
Ja

Begründung:
-

Umsetzung:
https://alamos-support.atlassian.net/wiki/x/woCq0w

Kapitel:
8 Technische Maßnahmen

Unterkapitel:
-

Maßnahmenziel:
Sicherstellung der erforderlichen Kapazität von Informationsverarbeitungseinrichtungen,

Personalwesen, Büros und anderen Einrichtungen.

Maßnahmen:
8.06 Kapazitätsmanagement

Massnahmentext:
Der Ressourceneinsatz sollte überwacht und entsprechend dem aktuellen und erwarteten Kapazitätsbedarf angepasst werden.

Anwendbarkeit:
Ja

Begründung:
-

Umsetzung:
https://alamos-support.atlassian.net/wiki/x/LgGr0w

Kapitel:
8 Technische Maßnahmen

Unterkapitel:
-

Maßnahmenziel:
Um sicherzustellen, dass Informationen und andere zugehörige Ressourcen vor Malware geschützt sind.

Maßnahmen:
8.07 Schutz vor Malware

Massnahmentext:
Der Schutz vor Malware sollte durch ein entsprechendes Benutzerbewusstsein implementiert und unterstützt werden.

Anwendbarkeit:
Ja

Begründung:
-

Umsetzung:
https://alamos-support.atlassian.net/wiki/x/vICp0w

Kapitel:
8 Technische Maßnahmen

Unterkapitel:
-

Maßnahmenziel:
Um die Ausnutzung technischer Schwachstellen zu verhindern.

Maßnahmen:

8.08 Management von technischen Schwachstellen

Massnahmentext:
Informationen über technische Schwachstellen der verwendeten Informationssysteme sollten eingeholt werden, die Exposition der Organisation gegenüber solchen Schwachstellen sollte bewertet und geeignete Maßnahmen ergriffen werden.

Anwendbarkeit:
Ja

Begründung:
-

Umsetzung:
https://alamos-support.atlassian.net/wiki/x/BoGr0w

Kapitel:
8 Technische Maßnahmen

Unterkapitel:
-

Maßnahmenziel:
Um sicherzustellen, dass Hardware, Software, Dienste und Netzwerke mit den erforderlichen Sicherheitseinstellungen ordnungsgemäß funktionieren und die Konfiguration nicht durch nicht autorisierte oder falsche Änderungen geändert wird.

Maßnahmen:
8.09 Konfigurationsverwaltung

Massnahmentext:
Konfigurationen, einschließlich Sicherheitskonfigurationen, von Hardware, Software, Diensten und Netzwerken sollten eingerichtet, dokumentiert, implementiert, überwacht und überprüft werden.

Anwendbarkeit:
Ja

Begründung:
-

Umsetzung:
https://alamos-support.atlassian.net/wiki/x/2YCp0w

Kapitel:
8 Technische Maßnahmen

Unterkapitel:
-

Maßnahmenziel:
Um eine unnötige Offenlegung sensibler Informationen zu vermeiden und gesetzliche, gesetzliche, regulatorische und vertragliche Anforderungen für die Löschung von Informationen einzuhalten.

Maßnahmen:
8.10 Löschen von Informationen

Massnahmentext:
Informationen, die in Informationssystemen, Geräten oder anderen Speichermedien gespeichert sind, sollten gelöscht werden, wenn sie nicht mehr benötigt werden.

Anwendbarkeit:
Ja

Begründung:
-

Umsetzung:
https://alamos-support.atlassian.net/wiki/x/MgCs0w

Kapitel:
8 Technische Maßnahmen

Unterkapitel:
-

Maßnahmenziel:
Um die Offenlegung sensibler Daten, einschließlich personenbezogener Daten, zu begrenzen und gesetzliche, gesetzliche, regulatorische und vertragliche Anforderungen einzuhalten.

Maßnahmen:
8.11 Regelungen zur Datenmaskierung (Anonymisierung und Pseudonomysierung)

Massnahmentext:
Die Datenmaskierung (Anonymisierung und Pseudonomysierung) sollte in Übereinstimmung mit den themenspezifischen Richtlinien der Organisation zur Zugriffskontrolle und anderen damit verbundenen themenspezifischen und geschäftlichen Anforderungen unter Berücksichtigung der geltenden Gesetze verwendet werden.

Anwendbarkeit:
Ja

Begründung:
-

Umsetzung:
https://alamos-support.atlassian.net/wiki/x/DoGr0w

Kapitel:
8 Technische Maßnahmen

Unterkapitel:
-

Maßnahmenziel:
Um die unbefugte Offenlegung und Extraktion von Informationen durch Einzelpersonen

oder Systeme zu erkennen und zu verhindern.

Maßnahmen:
8.12 Verhinderung von Datenlecks

Massnahmentext:
Maßnahmen zur Verhinderung von Datenlecks sollten auf Systeme, Netzwerke und alle anderen Geräte angewendet werden, die sensible Informationen verarbeiten, speichern oder übertragen.

Anwendbarkeit:
Ja

Begründung:
-

Umsetzung:
https://alamos-support.atlassian.net/wiki/x/34Cq0w

Kapitel:
8 Technische Maßnahmen

Unterkapitel:
-

Maßnahmenziel:
Um die Wiederherstellung nach Daten- oder Systemverlust zu ermöglichen.

Maßnahmen:
8.13 Informationssicherung

Massnahmentext:
Sicherungskopien von Informationen, Software und Systemen sollten in Übereinstimmung mit der vereinbarten themenspezifischen Sicherungsrichtlinie gepflegt und regelmäßig getestet werden.

Anwendbarkeit:
Ja

Begründung:
-

Umsetzung:
https://alamos-support.atlassian.net/wiki/x/5oCq0w

Kapitel:
8 Technische Maßnahmen

Unterkapitel:
-

Maßnahmenziel:
Sicherstellung des kontinuierlichen Betriebs von Informationsverarbeitungsanlagen.

Maßnahmen:
8.14 Redundanz von Informationsverarbeitungsanlagen

Massnahmentext:
Informationsverarbeitungsanlagen sollten mit Redundanzen implementiert werden, die ausreichen, um die Verfügbarkeitsanforderungen zu erfüllen.

Anwendbarkeit:
Ja

Begründung:
-

Umsetzung:
https://alamos-support.atlassian.net/wiki/x/6ICp0w

Kapitel:
8 Technische Maßnahmen

Unterkapitel:
-

Maßnahmenziel:
Um Ereignisse aufzuzeichnen, Beweise zu generieren, die Integrität von Protokollinformationen sicherzustellen, unbefugten Zugriff zu verhindern, Informationssicherheitsereignisse zu identifizieren, die zu einem Informationssicherheitsvorfall führen können, und Um Untersuchungen zu unterstützen.

Maßnahmen:
8.15 Protokollierung

Massnahmentext:
Protokolle, die Aktivitäten, Ausnahmen, Fehler und andere relevante Ereignisse aufzeichnen, sollten erstellt, gespeichert, geschützt und analysiert werden.

Anwendbarkeit:
Ja

Begründung:
-

Umsetzung:
https://alamos-support.atlassian.net/wiki/x/KYGr0w

Kapitel:
8 Technische Maßnahmen

Unterkapitel:
-

Maßnahmenziel:
Um anomales Verhalten und potenzielle Informationssicherheitsvorfälle zu erkennen.

Maßnahmen:

8.16 Überwachungstätigkeiten

Massnahmentext:
Netzwerke, Systeme und Anwendungen sollten auf anomales Verhalten überwacht und geeignete Maßnahmen ergriffen werden, um potenzielle Informationssicherheitsvorfälle zu bewerten.

Anwendbarkeit:
Ja

Begründung:
-

Umsetzung:
https://alamos-support.atlassian.net/wiki/x/wACm0w

Kapitel:
8 Technische Maßnahmen

Unterkapitel:
-

Maßnahmenziel:
Um die Korrelation und Analyse von sicherheitsrelevanten Ereignissen und anderen aufgezeichneten Daten zu ermöglichen und Untersuchungen zu Informationssicherheitsvorfällen zu unterstützen.

Maßnahmen:
8.17 Uhrensynchronisation

Massnahmentext:
Die Uhren der von der Organisation verwendeten Informationsverarbeitungssysteme sollten mit genehmigten Zeitquellen synchronisiert werden.

Anwendbarkeit:
Ja

Begründung:
-

Umsetzung:
https://alamos-support.atlassian.net/wiki/x/G4Gl0w

Kapitel:
8 Technische Maßnahmen

Unterkapitel:
-

Maßnahmenziel:
Um sicherzustellen, dass die Verwendung von Hilfsprogrammen die System- und Anwendungskontrollen für die Informationssicherheit nicht beeinträchtigt.

Maßnahmen:

8.18 Verwendung privilegierter Hilfsprogramme

Massnahmentext:
Die Verwendung von Hilfsprogrammen, die in der Lage sein können, System- und Anwendungskontrollen außer Kraft zu setzen, sollte eingeschränkt und streng kontrolliert werden.

Anwendbarkeit:
Ja

Begründung:
-

Umsetzung:
https://alamos-support.atlassian.net/wiki/x/GwGq0w

Kapitel:
8 Technische Maßnahmen

Unterkapitel:
-

Maßnahmenziel:
Gewährleistung der Integrität von Betriebssystemen und Verhinderung der Ausnutzung technischer Schwachstellen.

Maßnahmen:
8.19 Installation von Software auf Betriebssystemen

Massnahmentext:
Verfahren und Maßnahmen sollten implementiert werden, um die Softwareinstallation auf Betriebssystemen sicher zu verwalten.

Anwendbarkeit:
Ja

Begründung:
-

Umsetzung:
https://alamos-support.atlassian.net/wiki/x/RwCs0w

Kapitel:
8 Technische Maßnahmen

Unterkapitel:
-

Maßnahmenziel:
Schutz von Informationen in Netzwerken und ihren unterstützenden Informationsverarbeitungseinrichtungen vor einer Kompromittierung über das Netzwerk.

Maßnahmen:
8.20 Netzwerksicherheit

Massnahmentext:
Netzwerke und Netzwerkgeräte sollten gesichert, verwaltet und kontrolliert werden, um Informationen in Systemen und Anwendungen zu schützen.

Anwendbarkeit:
Ja

Begründung:
-

Umsetzung:
https://alamos-support.atlassian.net/wiki/x/IgGq0w

Kapitel:
8 Technische Maßnahmen

Unterkapitel:
-

Maßnahmenziel:
Um die Sicherheit bei der Verwendung von Netzwerkdiensten zu gewährleisten.

Maßnahmen:
8.21 Sicherheit von Netzwerkdiensten

Massnahmentext:
Sicherheitsmechanismen, Service-Level und Serviceanforderungen von Netzwerkdiensten sollten ermittelt, implementiert und überwacht werden.

Anwendbarkeit:
Ja

Begründung:
-

Umsetzung:
https://alamos-support.atlassian.net/wiki/x/KQGq0w

Kapitel:
8 Technische Maßnahmen

Unterkapitel:
-

Maßnahmenziel:
Um das Netzwerk in Sicherheitsgrenzen aufzuteilen und den Datenverkehr zwischen ihnen basierend auf den Geschäftsanforderungen zu steuern.

Maßnahmen:
8.22 Trennung von Netzwerken

Massnahmentext:
Gruppen von Informationdiensten, Benutzern und Informationssystemen sollten in den Netzwerken der Organisation getrennt werden.

Anwendbarkeit:
Ja

Begründung:
-

Umsetzung:
https://alamos-support.atlassian.net/wiki/x/M4Gr0w

Kapitel:
8 Technische Maßnahmen

Unterkapitel:
-

Maßnahmenziel:
Um Systeme vor Malware zu schützen und den Zugriff auf nicht autorisierte Webressourcen zu verhindern.

Maßnahmen:
8.23 Webfilterung

Massnahmentext:
Der Zugriff auf externe Websites sollte verwaltet werden, um das Risiko schädlicher Inhalte zu verringern.

Anwendbarkeit:
Ja

Begründung:
-

Umsetzung:
https://alamos-support.atlassian.net/wiki/x/IoGl0w

Kapitel:
8 Technische Maßnahmen

Unterkapitel:
-

Maßnahmenziel:
Gewährleistung einer ordnungsgemäßen und effektiven Verwendung der Kryptographie zum Schutz der Vertraulichkeit, Authentizität oder Integrität von Informationen gemäß den Geschäfts- und Informationssicherheitsanforderungen und unter Berücksichtigung gesetzlicher, gesetzlicher, regulatorischer und vertraglicher Anforderungen im Zusammenhang mit der Kryptographie.

Maßnahmen:
8.24 Einsatz von Kryptographie

Massnahmentext:
Regeln für den effektiven Einsatz von Kryptographie, einschließlich der kryptografischen Schlüsselverwaltung, sollten definiert und implementiert werden.

Anwendbarkeit:
Ja

Begründung:
-

Umsetzung:
https://alamos-support.atlassian.net/wiki/x/FYCt0w

Kapitel:
8 Technische Maßnahmen

Unterkapitel:
-

Maßnahmenziel:
Um die Informationssicherheit zu gewährleisten, wird sie innerhalb des sicheren Entwicklungslebenszyklus von Software und Systemen entworfen und implementiert.

Maßnahmen:
8.25 Sicherer Entwicklungslebenszyklus

Massnahmentext:
Es sollten Regeln für die sichere Entwicklung von Software und Systemen festgelegt und angewendet werden.

Anwendbarkeit:
Ja

Begründung:
-

Umsetzung:
https://alamos-support.atlassian.net/wiki/x/PIGo0w

Kapitel:
8 Technische Maßnahmen

Unterkapitel:
-

Maßnahmenziel:
Um sicherzustellen, dass alle Anforderungen an die Informationssicherheit bei der Entwicklung oder dem Erwerb von Anwendungen identifiziert und berücksichtigt werden.

Maßnahmen:
8.26 Anforderungen an die Anwendungssicherheit

Massnahmentext:
Anforderungen an die Informationssicherheit sollten bei der Entwicklung oder dem Erwerb von Anwendungen ermittelt, spezifiziert und genehmigt werden.

Anwendbarkeit:

Ja

Begründung:
-

Umsetzung:
https://alamos-support.atlassian.net/wiki/x/XACs0w

Kapitel:
8 Technische Maßnahmen

Unterkapitel:
-

Maßnahmenziel:
Um sicherzustellen, dass Informationssysteme innerhalb des Entwicklungslebenszyklus sicher entworfen, implementiert und betrieben werden.

Maßnahmen:
8.27 Sichere Systemarchitektur und Engineering-Prinzipien

Massnahmentext:
Grundsätze für die Entwicklung sicherer Systeme sollten festgelegt, dokumentiert, gepflegt und auf alle Tätigkeiten zur Entwicklung von Informationssystemen angewendet werden.

Anwendbarkeit:
Ja

Begründung:
-

Umsetzung:
https://alamos-support.atlassian.net/wiki/x/KYCt0w

Kapitel:
8 Technische Maßnahmen

Unterkapitel:
-

Maßnahmenziel:
Um sicherzustellen, dass Software sicher geschrieben wird, wodurch die Anzahl potenzieller Informationssicherheitsschwachstellen in der Software reduziert wird.

Maßnahmen:
8.28 Sichere Codierung im Entwicklungsprozess

Massnahmentext:
Sichere Codierungsprinzipien sollten auf die Softwareentwicklung angewendet werden.

Anwendbarkeit:
Ja

Begründung:
-

Umsetzung:
https://alamos-support.atlassian.net/wiki/x/2ACm0w

Kapitel:
8 Technische Maßnahmen

Unterkapitel:
-

Maßnahmenziel:
Um zu überprüfen, ob die Anforderungen an die Informationssicherheit erfüllt sind, wenn Anwendungen oder Code in der Produktionsumgebung bereitgestellt werden.

Maßnahmen:
8.29 Sicherheitstests in Entwicklung und Abnahme

Massnahmentext:
Sicherheitstestprozesse sollten im Entwicklungslebenszyklus definiert und implementiert werden.

Anwendbarkeit:
Ja

Begründung:
-

Umsetzung:
https://alamos-support.atlassian.net/wiki/x/ToCt0w

Kapitel:
8 Technische Maßnahmen

Unterkapitel:
-

Maßnahmenziel:
Um die informationssicherheit zu gewährleisten, werden die von der Organisation geforderten Maßnahmen in der ausgelagerten Systementwicklung implementiert.

Maßnahmen:
8.30 Ausgelagerte Entwicklung

Massnahmentext:
Die Organisation sollte die Aktivitäten im Zusammenhang mit der ausgelagerten Systementwicklung leiten, überwachen und überprüfen.

Anwendbarkeit:
Ja

Begründung:
-

Umsetzung:
https://alamos-support.atlassian.net/wiki/x/3wCm0w

Kapitel:
8 Technische Maßnahmen

Unterkapitel:
-

Maßnahmenziel:
Schutz der Produktionsumgebung und der Daten vor Kompromittierung durch Entwicklungs- und Testaktivitäten.

Maßnahmen:
8.31 Trennung von Entwicklungs-, Test- und Produktionsumgebungen

Massnahmentext:
Entwicklungs-, Test- und Produktionsumgebungen sollten getrennt und gesichert werden.

Anwendbarkeit:
Ja

Begründung:
-

Umsetzung:
https://alamos-support.atlassian.net/wiki/x/KIGp0w

Kapitel:
8 Technische Maßnahmen

Unterkapitel:
-

Maßnahmenziel:
Zur Wahrung der Informationssicherheit beim Ausführen von Änderungen.

Maßnahmen:
8.32 Veränderungsmanagement

Massnahmentext:
Änderungen an Informationsverarbeitungsanlagen und Informationssystemen sollten Änderungsmanagementverfahren unterliegen.

Anwendbarkeit:
Ja

Begründung:
-

Umsetzung:
https://alamos-support.atlassian.net/wiki/x/A4Cu0w

Kapitel:
8 Technische Maßnahmen

Unterkapitel:
-

Maßnahmenziel:
Sicherstellung der Testrelevanz und des Schutzes der für das Testen verwendeten Betriebsinformationen.

Maßnahmen:
8.33 Testinformationen

Massnahmentext:
Testinformationen sollten angemessen ausgewählt, geschützt und verwaltet werden.

Anwendbarkeit:
Ja

Begründung:
-

Umsetzung:
https://alamos-support.atlassian.net/wiki/x/L4Gp0w

Kapitel:
8 Technische Maßnahmen

Unterkapitel:
-

Maßnahmenziel:
Minimierung der Auswirkungen von Audit- und anderen Assurance-Aktivitäten auf Betriebssysteme und Geschäftsprozesse.

Maßnahmen:
8.34 Schutz von Informationssystemen bei Auditprüfungen

Massnahmentext:
Audit-Tests und andere Assurance-Aktivitäten, die eine Bewertung der Betriebssysteme beinhalten, sollten zwischen dem Tester und dem zuständigen Management geplant und vereinbart werden.

Anwendbarkeit:
Ja

Begründung:
-

Umsetzung:
https://alamos-support.atlassian.net/wiki/x/Y4Go0w
