Sicherheitsanforderungen von Alludo an Anbieter

Inhalt

Einleitung

Dieses Dokument beschreibt die Informationssicherheits-, Betriebskontinuitäts- und Datenschutzpraktiken der Unternehmen der Alludo-Gruppe (nachstehend zusammen „Alludo“ genannt) sowie das Programm zur Bewertung der Sicherheits- und Kontinuitätsmaßnahmen der Anbieter von Alludo. Die Prozesse, Verfahren, Anforderungen und Pflichten, auf die hierin verwiesen wird, werden nachstehend zusammen „Alludo-Standards“ genannt.

Dieses **Dokument zu den Sicherheitsanforderungen an Anbieter** informiert die Anbieter, die Waren und Dienstleistungen bereitstellen („Anbieter“), über die Sicherheits-, Betriebskontinuitäts- und Datenschutzerwartungen, für die sie von Alludo bei der Erbringung von Dienstleistungen verantwortlich gehalten werden. Anbieter müssen diese Anforderungen gemäß bester Praktiken und ihrer Unternehmenssicherheitsrichtlinien umsetzen. Alludo ist, ungeachtet der Ursache, nicht verantwortlich für Datenverluste, Geräteschaden oder sonstige Probleme der Anbieter.

Bei Widersprüchen zwischen diesem Dokument und einer schriftlichen Vereinbarung haben die Bestimmungen der schriftlichen Vereinbarung Vorrang. Anbieter müssen zudem alle lokalen, nationalen oder regionalen rechtlichen Anforderungen einhalten. Im Falle eines Konflikts zwischen diesem Dokument und geltenden Vorschriften müssen die Anbieter Alludo darüber in Kenntnis setzen und alternative Kontrollen vorschlagen, um gleichwertige Sicherheits-, Kontinuitäts- oder Datenschutzstandards zu wahren.

Übersicht über die Sicherheitsanforderungen an Anbieter

Alludo ist verpflichtet, seine vertraulichen und geheimen Informationen vor nicht autorisierter Verwendung oder Offenlegung zu schützen. Dazu setzt Alludo die Alludo-Standards um – interne Informationssicherheits-, Betriebskontinuitäts- und Datenschutzstandards, die gewährleisten, dass solche vertraulichen und geheimen Informationen geschützt sind und dass die von Alludo erbrachten Dienstleistungen kontinuierlich verfügbar sind. Um die Einhaltung der internen Standards und rechtlichen Anforderungen hinsichtlich der Informationssicherheit und Betriebskontinuität durch Alludo sicherzustellen, verlangt Alludo, dass seine Anbieter die in diesem Dokument beschriebenen Alludo-Standards beachten.

Wenn ein Anbieter einen Teil seiner Verpflichtungen im Rahmen seiner Vereinbarung mit Alludo überträgt oder untervergibt oder einen anderen Anbieter damit beauftragt, Alludo direkt oder indirekt Dienstleistungen zu erbringen, muss der Anbieter von einem solchen Anbieter verlangen, ein Informationsschutzprogramm umzusetzen und anzuwenden, das den Alludo-Standards entspricht. Alludo verpflichtet sich, mit seinen Anbietern in angemessener Weise zusammenzuarbeiten. um ihnen zu helfen, die Compliance-Anforderungen hinsichtlich der Alludo-Standards zu erfüllen. Der Geltungsbereich der Alludo-Standards für einen bestimmten Anbieter hängt von der Art der Dienstleistungen und Produkte ab, die der Anbieter Alludo bereitstellt.

Identitäts- und Zugangskontrolle

Der Anbieter muss Folgendes sicherstellen:

1. **Zugangskontrolle und Benutzerverwaltung**:
   - 1.1. Es ist eine dokumentierte Zugriffskontrollrichtlinie vorhanden, die mindestens einmal jährlich überprüft wird.
   - 1.2. Die Rollen, Genehmigungen und Zugriffsrechte der Benutzer werden definiert und dokumentiert.
   - 1.3. Es sind Standardverfahren für das Onboarding und Offboarding von Benutzern vorhanden, einschließlich des Führens von Aufzeichnungen über die relevanten Genehmigungen.
   - 1.4. Der Zugriff auf die IT-Infrastrukturkomponenten wird nach dem Prinzip der minimalen Berechtigung gewährt und über Identitätsmanagement-Tools (z. B. Active Directory, OKTA oder ähnliche Tools) verwaltet.

1.5. Der individuelle Zugang zu Systemen, Netzwerkressourcen und sonstigen IT-Ressourcen wird formell über eindeutige Benutzer-IDs und individuelle Kennwörter genehmigt und gesteuert.
1.6. Während der Erstellung/Änderung von Benutzer-IDs und der Zuweisung von Rechten wird eine Trennung der Aufgabenbereiche aufrecht erhalten.

2. **Kennwort- und Authentifizierungsrichtlinien**:
   2.1. Es wird von den Benutzern verlangt, dass Sie nach ihrer ersten Anmeldung ihr Kennwort ändern.
   2.2. Die Kennwörter entsprechen hinsichtlich Länge, Ablaufdatum, Komplexität, Kennwortverlauf, gescheiterte Versuche, Kontosperrdauer, Kennwortalter und Änderung nach der ersten Anmeldung den branchenüblichen Standards.
   2.3. Vor der Zurücksetzung von Kennwörtern kommen sichere Mechanismen zur Bereitstellung der Benutzerkennwörter und Überprüfung von Benutzeridentitäten zum Einsatz.
   2.4. Systeme, die IdP-Authentifizierung nicht unterstützen oder die unabhängig erstellt werden müssen, werden so konfiguriert, dass eine strenge Authentifizierung durchgesetzt wird, wobei mindestens die in den zentralen Kennwort- und Zugriffskontrollrichtlinien definierte Konfiguration angewendet wird.
   2.5. Alle Systeme und Anwendungen werden so konfiguriert, dass sichere Anmeldeverfahren über genehmigte Identitäts- und Zugriffsmanagement-Mechanismen zur Anwendung gelangen.
   2.6. Um einen nicht autorisierten Zugriff zu verhindern, werden Systeme und Anwendungen so konfiguriert, dass inaktive Sitzungen nach einer bestimmten Zeit beendet werden.

3. **Verwaltung des privilegierten Zugangs**:
   3.1. Der privilegierte Zugang zu Ressourcen ist auf definierte Benutzerrollen beschränkt und wird von dazu berechtigten Mitarbeitern genehmigt.
   3.2. Privilegierte Benutzerkonten werden so konfiguriert, dass eine Multifaktor-Authentifizierung zum Einsatz kommt.
   3.3. Privilegien, die nicht mehr benötigt werden, werden sofort widerrufen.
   3.4. Die Verwendung von Administratorrechten ist auf bestimmte Fälle, wie die Fehlerbehebung, beschränkt, und zur Durchführung der Tagesgeschäfte verwenden die Benutzer geringstprivilegierte Anmeldeinformationen.
   3.5. Der Zugriff auf die IT-Infrastruktur, Systeme, Netzwerkgeräte und Anwendungen (z. B. Remote-Zugriff, kritische Server, Netzwerk-Geräte) ist durch eine Multifaktor-Authentifizierung geschützt.

4. **Zugangsüberprüfung und -überwachung**:
   4.1. Es werden regelmäßige Überprüfungen der Zugriffsrechte durchgeführt und erkannte Abweichungen werden umgehend behoben.
   4.2. Nicht mehr als jährlich wird ein Abgleich aller Benutzer-IDs (einschließlich Domain, Anwendungen, Netzwerkgeräte, IT-Systeme, Middleware, Datenbanken usw.) durchgeführt. Es werden sofort Korrekturmaßnahmen ergriffen, wenn Abweichungen erkannt werden.
5. **Management von Drittunternehmen und Anbietern**:

5.1. Der Zugriff von Drittparteien auf Netzwerke und Systeme wird streng kontrolliert, formell genehmigt und erfolgt nach dem Need-to-know-Prinzip.
5.2. Vom Anbieter bereitgestellte Standard-Anmeldeinformationen werden geändert, bevor Systeme, Anwendungen, Netzwerkgeräte oder andere IT-Infrastrukturgeräte eingeführt werden.

6. **Sonderzugangserwägungen**:
   6.1. Allgemeine und gemeinsam genutzte IDs werden nur genutzt, wenn sie von der Geschäftsleitung formal begründet und genehmigt wurden und über Mechanismen verfügen, um die Nutzung und alle Aktionen zu einzelnen Benutzern zurückzuverfolgen.
   6.2. Jeglicher Nicht-Konsolen-Administratorzugriff wird unter Verwendung branchenbewährter Verschlüsselungsalgorithmen verschlüsselt, und unsichere Protokolle (z. B. telnet/ftp) sind für Nicht-Konsolen-Administratorzugriffe verboten.

Ressourcen-Verwaltung

Der Anbieter muss Folgendes sicherstellen:

7. **Ressourcen-Verwaltung und -inventur**:
   7.1. Es werden umfassende Ressourcen-Bestandsverzeichnisse geführt, in denen wesentliche Angaben wie Informationen zum Ressourcen-Inhaber, Kontaktdaten und Speicherort erfasst werden.
   7.2. Um die Richtigkeit der Datensätze der Informationstechnologie-Ressourcen, wie Hardware, Betriebssysteme, Anwendungen und Datenbanken, zu gewährleisten, werden diese regelmäßig aktualisiert und überprüft.
   7.3. Es werden Ressourcen-Verwaltungsverfahren und Konfigurationskontrollen zur Verwaltung der Verfügbarkeit kritischer Ressourcen und der Konfigurationen entscheidender Netz- und Informationssysteme eingeführt und eingehalten.

8. **Informationsklassifikation und -kennzeichnung**:
   8.1. Es wird eine Richtlinie zur Informationsklassifikation mit den entsprechenden Verfahren und Leitlinien angewendet. Alle Ressourcen werden nach festgelegten Anweisungen gekennzeichnet und die Informationen werden aufgrund definierter Klassifizierungsstufen klassifiziert und geschützt.

9. **Ressourcen-Handling**:
   9.1. Für eine ordnungsgemäße Abwicklung werden Leitlinien zur Ressourcen-Verwaltung befolgt und allen betroffenen Mitarbeitern und Auftragnehmern kommuniziert.
   9.2. Es bestehen dokumentierte Verfahren für den Schutz von Ressourcen-Beständen, zur Identifizierung von Ressourcen, die entsorgt werden müssen, und zur Gewährleistung einer sicheren Entsorgung solcher Ressourcen.
   9.3. Es werden Prozesse eingeführt, um sicherzustellen, dass zugeordnete Ressourcen nach der Beendigung oder dem Ausscheiden aus einem Arbeitsverhältnis, einer Vertragsauflösung oder einer Kündigung eines Vertrages unverzüglich dem zuständigen Ressourcen-Verwaltungs-Team zurückgegeben werden.

10. **Verwaltung von Mobilgeräten und Wechselmedien**:
    10.1. Es werden Richtlinien und Verfahren zur Kontrolle von Mobilgeräten (einschließlich BYOD) eingeführt, die zur Speicherung, Übertragung oder Verarbeitung von Geschäftsinformationen verwendet werden. Es sind angemessene Schutzmaßnahmen erforderlich, bevor Mobilgeräten erlaubt wird, auf Geschäftsinformationen und Ressourcen zuzugreifen.
    10.2. Die Verwendung von austauschbaren Massenspeichergeräten muss zur Gewährleistung der Datensicherheit verschlüsselt werden.

11. **Software-Compliance**:
    11.1. Die Verwendung unlizenzierter oder nicht genehmigter Software ist verboten. Es gibt Verfahren, um Verstöße zu erkennen und notwendige Maßnahmen zu deren Unterbindung zu treffen.

IT-Betrieb

Der Anbieter muss Folgendes sicherstellen:

12. **Betrieb kritischer Systeme**:
    12.1. Es werden Verfahren für den Betrieb kritischer Netz- und Informationssysteme eingeführt und befolgt, die Folgendes umfassen:
        12.1.1. Formelle Genehmigungsprozesse für den Zugriff auf IT-Ressourcen
        12.1.2. Zuverlässige Authentisierungsmechanismen für alle Technologien (z. B. VPN, Windows-Anmeldung)
        12.1.3. Regelmäßige Überprüfung des Anspruchs auf Privilegien
        12.1.4. Identifizierung von Netzwerkspeicherorten für kritische Technologien aufgrund von Betriebskontinuitätsanforderungen

13. **Veränderungsmanagement**:
    13.1. Es wird ein umfassender Veränderungsmanagement-Prozess für IT-Systeme, Anwendungen, Datenbanken und Netzwerk-Komponenten implementiert, um Folgendes zu gewährleisten:
        13.1.1. Protokollierung, Überprüfung, Testen und formelle Genehmigung aller Änderungen
        13.1.2. Rollback-Pläne für potenziell störende Änderungen

14. **Sonstiges**:
    14.1. Bei Systemen und Netzwerk-Komponenten, die sensible und vertrauliche Informationen verarbeiten, wird die Dateiintegritätsüberwachung geprüft.
    14.2. Alle Systeme und Netzwerk-Komponenten werden so konfiguriert, dass sie für eine akkurate Zeitsynchronisierung autorisierte Network-Time-Protocol-Quellen (NTP) verwenden.
    14.3. Für alle kritischen Systeme, Anwendungen, Netzwerkgeräte und Endbenutzer-Maschinen werden regelmäßige proaktive und vorbeugende Instandhaltungsprozesse eingerichtet.

14.4. Die Firewall- und Router-Regelsätze werden regelmäßig oder nach Branchenstandards überprüft und unnötige oder unerlaubte Regeln werden umgehend entfernt.
14.5. Es werden Kontrollen implementiert, um die Integrität von Informationen und Software in der ganzen IT-Umgebung aufrecht zu erhalten.

Sicherheit im Personalwesen

Der Anbieter muss Folgendes sicherstellen:

15. **Hintergrundprüfungen**:
    15.1. Es werden Richtlinien und Verfahren zur Durchführung von Hintergrundprüfungen festgelegt und aufrecht erhalten.
    15.2. Es werden, soweit gesetzlich zulässig, vor dem Onboarding angemessene Hintergrundprüfungen der Mitarbeiter und Auftragnehmer aufgrund ihrer Aufgaben und Verantwortlichkeiten durchgeführt.
16. **Personalveränderungsmanagement**:
    16.1. Es wird ein Prozess zur Verwaltung der Änderungen des Personals oder dessen Rollen und Verantwortlichkeiten implementiert, einschließlich der Schulung neuer Mitarbeiter in den relevanten Richtlinien und Verfahren.
    16.2. Zugriffsrechte, Ausweise, Geräte und andere Ressourcen werden bei Personaländerungen umgehend entzogen, falls sie nicht mehr erforderlich oder nicht mehr zulässig sind.
17. **Richtlinien-Durchsetzung**:
    17.1. Für Mitarbeiter, die gegen Sicherheitsrichtlinien verstoßen, wird ein klares Disziplinarverfahren eingeführt und aufrechterhalten.
    17.2. Durch angemessene vertragliche Maßnahmen wird die Rechenschaftspflicht für Verstöße gegen Sicherheitsrichtlinien sichergestellt. Dazu gehört die Aufnahme einschlägiger Bestimmungen in die Arbeitsverträge für Mitarbeiter und die Dienstleistungsverträge für Auftragnehmer.

Sicherheits- und Datenschutzschulung

Der Anbieter muss Folgendes sicherstellen:

18. Sicherheits- und Datenschutzschulungen sind für alle Mitarbeiter und Auftragnehmer verpflichtend. Diese Schulungen müssen bei der Einstellung und anschließend jährlich oder weniger häufig absolviert werden.
19. Mitarbeiter und Auftragnehmer mit bedeutenden IT-Sicherheitsaufgaben müssen spezialisierte jährliche Schulungen absolvieren, die auf ihre spezifische Rolle und Aufgabe zugeschnitten sind.
20. Die Geschäftsleitung hat Zugriff auf Tools und Systeme, die es ihr erlauben, die Schulungsfortschritte ihrer Mitarbeiter und Auftragnehmer zu überwachen und zu verfolgen.
21. Das Schulungs- und Sensibilisierungsprogramm des Unternehmens wird regelmäßig überprüft und aktualisiert. Dabei werden die sich wandelnden Geschäftsanforderungen, rechtliche Änderungen und aus vergangenen Sicherheitsvorfällen gewonnene Erkenntnisse berücksichtigt.

Informationssicherheit und -Governance

Der Anbieter muss Folgendes sicherstellen:

22. **Sicherheits-Framework und -Governance**:
    - 22.1. Der Anbieter muss ein anerkanntes Sicherheitsstandard-Framework (z. B. NIST CSF, RMF, 800-53, ISO 27001, CIS) zur Informations- und Cybersicherheits-Governance implementieren. Das Framework sollte Folgendes umfassen:
        - 22.1.1. Umfassende Informations- und Cybersicherheits-Richtlinien und -verfahren, die jährlich überprüft, formell genehmigt und unternehmensweit kommuniziert werden
        - 22.1.2. Eine klar definierte und auf die Geschäftsziele abgestimmte Informationssicherheitsstrategie
        - 22.1.3. Robuste Governance- und Risikomanagementprozesse, die spezifisch Informations- und Cybersicherheitsrisiken angehen
        - 22.1.4. Compliance-Mechanismen zur Einhaltung der rechtlichen und regulatorischen Anforderungen an Informationen und Cybersicherheit
    - 22.2. Wenn kein anerkanntes Sicherheits-Framework angewendet wird, muss der Anbieter einen Bericht vorlegen, der nachweist, dass die Umgebung einer Prüfung unterzogen wurde.
        - 22.2.1. Zwischen dem Anbieter und Alludo sollte ein Abhilfeplan für erkannte Probleme, einschließlich des erwarteten Zeitrahmens, vereinbart werden.

23. **Führungs- und Unternehmensstruktur:**
    - 23.1. Es werden im ganzen Unternehmen angemessene Rollen und Aufgaben für die Informations- und Cybersicherheit definiert und übertragen.

24. **Risikomanagement und -bewertung:**
    - 24.1. Es ist ein formelles, von der höheren Führungsebene genehmigtes Risikomanagement-Framework vorhanden:
        - 24.1.1. zur Erkennung sowohl interner als auch externer Bedrohungen
        - 24.1.2. zur Bewertung der Sensibilität von Informationen/Daten
        - 24.1.3. zur Beurteilung möglicher Auswirkungen auf das Geschäft
        - 24.1.4. zur Bewertung von Bedrohungen, Schwachstellen und entsprechenden Risiken
            - 24.1.4.1. Alle identifizierten Risiken und Bedrohungen werden priorisiert und es werden zeitnah Maßnahmen getroffen, um die Risiken entsprechend zu vermindern.
            - 24.1.4.2. Es werden Prozesse und/oder Tools implementiert, um Ereignisse zu erkennen, die zu Unterbrechungen von zentralen Geschäftszwecken des Unternehmens führen könnten.
            - 24.1.4.3. Der Anbieter muss Alludo umgehend benachrichtigen, wenn er nicht in der Lage ist, ein wesentliches Risiko zu beseitigen oder zu verringern, das sich auf die erbrachten Dienstleistungen auswirken könnte.

25. **Compliance- und Leistungsüberwachung:**
    - 25.1. Es sind Prozesse in Kraft, um alle geltenden rechtlichen, regulatorischen und vertraglichen Anforderungen des Unternehmens zu identifizieren, zu erfassen und zu verfolgen.

25.2. Es werden regelmäßige Prüfungen durchgeführt, um die Einhaltung rechtlicher, regulatorischer und vertraglicher Verpflichtungen zu bestätigen. Es werden Aufzeichnungen dieser Bewertungen geführt und erkannte Lücken werden unverzüglich behoben.
25.3. Die Richtlinien, Verfahren und Leitlinien werden mindestens jährlich gemäß der rechtlichen, regulatorischen und vertraglichen Anforderungen überprüft und aktualisiert.
25.4. Es werden Leistungsindikatoren für kritische Funktionen wie IT, Informationssicherheit und Datenschutz usw. definiert, offiziell dokumentiert, regelmäßig bewertet und der Geschäftsleitung gemeldet.

Netzwerk-Sicherheit

Der Anbieter muss Folgendes sicherstellen:

26. Netzwerkdesign und Sicherheitsarchitektur:

26.1. Das Netzwerk des Anbieters beruht auf den Grundsätzen der „gestaffelten Sicherheitsebenen“ und beinhaltet geeignete Kontrollen wie die Segmentierung des Netzwerks, um Verletzungen der Informations- und Cybersicherheit zu minimieren.
26.2. Es wird ein solides architektonisches Design mit einem effektiven Identitätsmanagement und robusten Betriebssystemkonfigurationen implementiert.
26.3. Das Netzwerkdesign und seine Implementierung werden jährlich überprüft, um andauernde Wirksamkeit und Sicherheit zu gewährleisten.
26.4. Die Netzkonfiguration entspricht allen geltenden rechtlichen und regulatorischen Anforderungen.

27. Zugangskontrolle und Authentifizierung:

27.1. Externe Netzwerkverbindungen müssen dokumentiert, durch Firewalls geleitet, überprüft und genehmigt werden, bevor sie eingerichtet werden.
27.2. Der drahtlose Netzwerkzugang erfordert Authentifizierung, Autorisierung, Segmentierung und Verschlüsselung. Es sind Systeme vorhanden, die nicht autorisierte drahtlose Zugangspunkte oder nicht autorisierte Verbindungen erkennen und darauf reagieren.
27.3. Der Fernzugriff auf das Netzwerk des Anbieters muss genehmigt werden und auf sichere Weise mit mehrstufiger Authentifizierung erfolgen.
27.4. Es werden Kontrollen implementiert, um den unbefugten Zugriff auf das Netzwerk des Anbieters zu verhindern oder zu minimieren.

28. Sichere Administration und Verwaltung:

28.1. Für den gesamten verwaltungsbezogenen Netzwerkverkehr zwischen den administrativen Arbeitsplätzen und den Netzwerkgeräten werden branchenübliche Verschlüsselungs- und Authentifizierungsprotokolle verwendet.
28.2. Der Nicht-Konsolen-Administratorzugriff erfolgt ausschließlich über branchenübliche, verschlüsselte Kanäle.
28.3. Gastkonten werden deaktiviert oder entfernt und alle Standard- und vom Anbieter bereitgestellten Kennwörter werden geändert, bevor die Netzwerkgeräte in der Produktionsumgebung eingesetzt werden.

29. **Netzwerkhärtung und Schutz vor Bedrohungen:**
    29.1. Nicht genutzte Dienste, Anwendungen und Ports werden deaktiviert, um die Angriffsfläche zu verringern.
    29.2. Für kritische Netzsegmente werden Maßnahmen zur Angriffserkennung und/oder -verhinderung eingesetzt.
    29.3. Kritische Systeme sind gegen Denial-of-Service- (DoS) und Distributed-Denial-of-Service-Angriffe (DDoS) geschützt.

Kryptographie

Der Anbieter muss Folgendes sicherstellen:

30. Es wird eine umfassende Kryptografie-Richtlinie zusammen mit entsprechenden Verfahren implementiert, um die Einhaltung aller relevanten rechtlichen, regulatorischen und geschäftlichen Anforderungen zu gewährleisten. Diese Richtlinie folgt bewährten Verfahren, um eine sichere Verschlüsselung in Übereinstimmung mit den geltenden Gesetzen und Normen zu gewährleisten.

31. **Verschlüsselungsstandards und -implementierung**:
    31.1. Es sind nur sichere, in der Branche zugelassene Verschlüsselungsalgorithmen und Schlüsselstärken zulässig, die einen angemessenen, system- und prozessübergreifenden Datenschutz gewährleisten.
    31.2. Zum Schutz vertraulicher Informationen und zur Beschränkung des Zugangs zu sensiblen Daten werden kryptografische Lösungen eingesetzt. Daten werden sowohl bei der Übertragung als auch im Ruhezustand verschlüsselt.
    31.3. Die gesamte Speicherung und die Übertragung von Kennwörtern erfolgen verschlüsselt, so dass die Vertraulichkeit der Benutzerdaten jederzeit gewährleistet ist.
    31.4. Die Daten von Alludo müssen bei der Übertragung verschlüsselt werden (mindestens TLS 1.2 oder ein neuerer Standard).
    31.5. Daten von Alludo im Ruhezustand müssen verschlüsselt werden (mindestens AES 256-Bit oder ein neuerer Standard).

Datensicherheit

Der Anbieter muss Folgendes sicherstellen:

32. **Wiederherstellung:**
    32.1. **Datensicherung und -wiederherstellung**:
        32.1.1. Es müssen regelmäßig Backups der Daten von Alludo erstellt werden.
        32.1.2. Die Backups der Daten von Alludo müssen 1 Jahr aufbewahrt werden.
        32.1.3. Die Backups der Daten von Alludo müssen verschlüsselt werden.
    32.2. **Disaster Recovery**:
        32.2.1. Der Disaster-Recovery-Plan muss jährlich getestet werden.

33. **Backup-Richtlinie und Verfahren**:

33.1. Die Backup-Richtlinie und die entsprechenden Verfahren müssen klar dokumentiert werden.
33.2. Die Backup-Wiederherstellungsprozesse müssen dokumentiert und regelmäßig getestet werden.
33.3. Die Nachweise der Backup-Wiederherstellungstests müssen aufbewahrt werden.
33.4. Von kritischen Datenbackup-Dateien muss eine Kopie gesichert aufbewahrt werden.

34. **Backup-Überwachung**:
34.1. Die Protokolle etwaiger fehlgeschlagener Backups müssen von den Backup-Administratoren überwacht werden.
34.2. Für fehlgeschlagene Backups müssen Korrekturmaßnahmen durchgeführt und dokumentiert werden.

35. **Datenspeicherort**:
35.1. Der Anbieter ist dafür verantwortlich, dass in den Ländern, in denen die Daten gespeichert werden, alle geltenden Datenschutzgesetze eingehalten werden.
35.2. Einhaltung der Beschränkungen für die grenzüberschreitende Datenübermittlung (DSGVO usw.).
35.3. Der Anbieter muss angemessene technische und organisatorische Sicherheitsmaßnahmen zum Schutz der Daten ergreifen, die den Gesetzen und Normen der Länder entsprechen, in denen die Daten gespeichert sind.
35.4. Alludo behält sich das Recht vor, die Datenverarbeitungspraktiken des Anbieters zu überprüfen, um die Einhaltung der vereinbarten Sicherheitsmaßnahmen und der örtlichen Vorschriften sicherzustellen.

36. **Löschen von Daten**:
36.1. Es müssen Verfahren zur sicheren Datenlöschung bei Vertragsbeendigung vorhanden sein, die die Einhaltung der lokalen Gesetze zur Vorratsdatenspeicherung gewährleisten.

37. **Festplattenverschlüsselung**:
37.1. Für Workstations und Server muss eine Festplattenverschlüsselung eingerichtet werden.

38. **Datenklassifizierung**:
38.1. Es muss eine dokumentierte Datenklassifizierungsrichtlinie vorhanden sein.
38.2. Die Daten müssen nach ihrer Kritikalität und Sensibilität klassifiziert werden.
38.3. Es müssen Sicherheitskontrollen identifiziert und implementiert werden, die der Sensibilität der Daten entsprechen.

Informationskommunikation

Der Anbieter muss Folgendes sicherstellen:

39. **Web-Sicherheit**:
39.1. Es wird Software zur Filterung von Webinhalten eingesetzt, um den Zugang zu Websites mit schädlichen Inhalten zu blockieren.

39.2. Der Zugriff auf alle webbasierten Systeme und Anwendungen muss über sichere und authentifizierte Mechanismen erfolgen.
39.3. Die Client-Server-Kommunikation für Anwendungen und Webportale muss über verschlüsselte Kanäle erfolgen.

40. E-Mail-Sicherheit:
40.1. Es sind Sicherheitskontrollen zur Verhinderung des Missbrauchs des E-Mail-Systems in Kraft.
40.2. Die gesamte E-Mail-Kommunikation muss über verschlüsselte Kanäle erfolgen.
40.3. Das E-Mail-Gateway ist mit Folgendem ausgestattet:
40.3.1. Anti-Phishing-Filter
40.3.2. aktivierte Sicherheitsprotokolle für E-Mails (z. B. DMARC, DKIM und SPF)
40.3.3. sonstige notwendige Konfigurationen, um E-Mail-Bedrohungen zu verhindern

Software-Entwicklung

Der Anbieter muss Folgendes sicherstellen:

41. Softwareentwicklungslebenszyklus:
41.1. Es muss ein etablierter Rahmen für die Software- und Systementwicklung vorhanden sein.
41.2. Systeme und Anwendungen müssen nach bewährten Verfahren für die sichere Softwareentwicklung (z. B. OWASP) entwickelt werden.
41.3. Software-Code muss:
41.3.1. vor unbefugter Änderung geschützt sein
41.3.2. sicher gespeichert sein
41.3.3. Qualitätssicherungsprozessen unterworfen sein
41.4. Es müssen Code-Reviews durchgeführt werden.

42. Testen und Bereitstellung:
42.1. Anwendungen müssen vor dem Einsatz in der Produktionsumgebung gründlichen Sicherheits- und Funktionstests unterzogen werden.
42.2. Produktions- und Nicht-Produktionsumgebungen müssen angemessen voneinander getrennt werden.
42.3. Die Aufgabentrennung zwischen Produktions- und Nicht-Produktionsentwicklung muss beibehalten werden.
42.4. In einer Testumgebung dürfen keine Produktionsdaten vorhanden sein.

Anwendungssicherheit

Der Anbieter muss Folgendes sicherstellen:

43. Anwendungssicherheit:
43.1. Für alle neu entwickelten und für alle bestehenden Anwendungen, an denen wesentliche Änderungen vorgenommen werden, werden Anwendungssicherheitsbewertungen durchgeführt, um bekannte Sicherheitslücken zu ermitteln.

43.2. Alle identifizierten Sicherheitslücken mit einem CVSS-Wert von mehr als 4 werden beseitigt, bevor die Anwendung in der Produktionsumgebung eingesetzt wird.

43.3. Es werden Verfahren zur Code-Review implementiert, um Code zu identifizieren und zu korrigieren, der Sicherheitslücken schaffen könnte.

44. Schutz von Webanwendungen:

44.1. Öffentlich zugängliche Webanwendungen werden durch eine robuste Webanwendungsfirewall geschützt, um externe Bedrohungen abzuwehren.

Patch-Verwaltung

Der Anbieter muss Folgendes sicherstellen:

45. Die neuesten Sicherheits-Patches werden zeitnah und in Abhängigkeit von der Kritikalität der mit dem Patch behobenen Schwachstelle auf Systeme, Netzwerke, Anwendungen, Datenbanken usw. aufgespielt. Für proprietäre Systeme werden die Patches direkt von den jeweiligen OEMs bezogen.

46. Alle Patches werden getestet, bevor sie auf die Produktionssysteme aufgespielt werden, und nach jedem Patching wird der korrekte Betrieb des gepatchten Dienstes überprüft.

47. Für den Fall, dass ein System nicht gepatcht werden kann, werden geeignete Abhilfemaßnahmen ergriffen. Die Wirksamkeit dieser Abhilfemaßnahmen wird regelmäßig bewertet und entsprechende Nachweise werden aufbewahrt.

Malware-Schutz

Der Anbieter muss Folgendes sicherstellen:

48. Alle IT-Systeme werden stets durch eine Lösung zum Schutz vor Malware geschützt, die eingehende Daten in Echtzeit prüft, um Serviceunterbrechungen oder Sicherheitsverletzungen zu verhindern. Außerdem werden angemessene Verfahren zur Sensibilisierung der Benutzer durchgesetzt. Das Anti-Malware-System erkennt verschiedene Bedrohungen, insbesondere Viren, Spyware, Würmer, nicht autorisierter mobiler Code, Keylogger, Botnets und Trojaner.

49. Malware-Signaturen werden regelmäßig aktualisiert, um sicherzustellen, dass die Systeme immer mit den neuesten Bedrohungsdefinitionen ausgestattet sind.

50. Die Software zum Schutz vor Malware ist so konfiguriert, dass sie sowohl geplante als auch On-Demand-Scans durchführt und erkannte schädliche Dateien oder schädliche Software isoliert oder löscht.

51. Endbenutzer verfügen weder über die Rechte noch die Möglichkeit, den Malware-Schutz zu deaktivieren.

Schwachstellenmanagement

Der Anbieter muss Folgendes sicherstellen:

52. Schwachstellenmanagement-Prozess:

52.1. Bestehende Richtlinien, Prozesse und Verfahren für ein umfassendes Schwachstellenmanagement.
52.2. Verfahren zum Empfang, zur Analyse und zur Reaktion auf Schwachstellen aus internen und externen Quellen.

53. Bewertung und Behebung von Schwachstellen:
53.1. Vierteljährliche Schwachstellenbewertung der IT-Infrastruktur und der Anwendungen des Anbieters, einschließlich der Disaster-Recovery-Websites.
53.2. Behebung erkannter Schwachstellen mit einem CVSS-Wert von über 4 innerhalb festgelegter Fristen.

54. Penetrationstests:
54.1. Jährliche unabhängige Penetrationstests der IT-Infrastruktur des Anbieters und der für die Alludo-Dienste genutzten Anwendungen.
54.2. Die Tests zielen darauf ab, ausnutzbare Schwachstellen zu erkennen und Sicherheitsverletzungen durch Cyberangriffe zu verhindern.
54.3. Alludo gewährt auf begründeten Antrag Zugang zu den einschlägigen Berichten über Penetrations- und Schwachstellentests.

Protokollierung und Überwachung

Der Anbieter muss Folgendes sicherstellen:

55. Kritische Systeme, einschließlich Anwendungen, sind so eingestellt, dass sie wichtige Ereignisse (einschließlich privilegierter Zugriffe und Benutzeraktivitäten) protokollieren und für einen Zeitraum von mindestens einem Jahr oder gemäß den geltenden gesetzlichen Bestimmungen aufbewahren.
56. Die Protokolle von Schlüsselereignissen enthalten (soweit erforderlich) mindestens Folgendes:
56.1. Systemstart und -abschaltung
56.2. Start- und Stopp-Status von kritischen Diensten und Prozessen
56.3. Änderungen der Konfigurationsparameter, z. B. Änderungen der Systemstartkonfiguration
56.4. Erfolgreiche Anmeldungen und fehlgeschlagene Anmeldeversuche
56.5. Erstellung, Änderung und Löschung von Benutzerkonten
56.6. System/Ressourcen, auf die zugegriffen wird
56.7. Identifizierung und Lokalisierung der Personen, die auf die Ressourcen zugegriffen haben, und des Ortes, von dem aus auf die Ressourcen zugegriffen wurde
56.8. Datum und Zeitstempel
57. Es werden Audit-Protokolle von mehreren Quellen und Sensoren gesammelt und korreliert, sicher gespeichert und vor Manipulationen geschützt, um die Rekonstruktion solcher Ereignisse zu ermöglichen.
58. Es werden Prozesse zur Überwachung von Protokollereignissen (vorzugsweise in Echtzeit) eingerichtet, um unbefugte Aktivitäten und Angriffsziele zu erkennen und sicherzustellen, dass die Protokolle der wichtigsten Ereignisse überprüft werden.

Störfallmanagement

Der Anbieter muss Folgendes sicherstellen:

59. Es sind klare Rollen und Prozesse definiert, um eine prompte, effektive und organisierte Reaktion auf Vorfälle im Bereich der Informationssicherheit und des Datenschutzes zu gewährleisten.

60. Mitarbeiter und Auftragnehmer sind auf die Erkennung von Sicherheitsvorfällen geschult und wissen, wie und wo sie potenzielle oder bestätigte Vorfälle melden sollen.

61. Das für die Analyse der Vorfälle und die entsprechende Reaktion zuständige Personal ist entsprechend qualifiziert und wird regelmäßig in wirksamen Verfahren zur Reaktion auf Vorfälle geschult.

62. Es wird ein Verzeichnis für alle gemeldeten Vorfälle geführt, in dem die Maßnahmen zur Minderung der Auswirkungen des Vorfalls und die aus dem Vorfall gezogenen Lehren beschrieben sind.

63. Alludo wird benachrichtigt, sobald das Unternehmen von einem Sicherheitsvorfall erfährt, der Alludo betrifft, spätestens jedoch 24 Stunden nach der Entdeckung.

Physische und umgebungsbezogene Sicherheit

Der Anbieter muss Folgendes sicherstellen:

64. Es werden Richtlinien und Verfahren für die physische Sicherheit und Umweltkontrollen umgesetzt, die den Industriestandards entsprechen.

65. Kritische Einrichtungen, in denen IT-Systeme, -Anwendungen und -Personal untergebracht sind (z. B. Rechenzentren, Betriebsstätten), werden vor Unfällen, Angriffen und unberechtigtem Zugriff geschützt.

66. Es sind Sicherheitsmaßnahmen wie elektronische Zugangskontrollen, Identitätsüberprüfung, Sicherheitspersonal, Besuchermanagement und Videoüberwachung rund um die Uhr vorhanden, um einen unbefugten Zutritt zu verhindern.

67. Die Aufnahmen der Videoüberwachung werden mindestens 30 Tage lang aufbewahrt, oder länger, wenn es die gesetzlichen Bestimmungen erfordern.

68. Der Zugang zu den Einrichtungen ist auf befugtes Personal für bestimmte Zwecke beschränkt und wird regelmäßig überprüft.

69. Besucher werden begleitet, der Zeitpunkt des Betretens und Verlassens der Einrichtung protokolliert und sie müssen jederzeit einen Besucherausweis tragen. Zugangskarten oder Schlüssel werden bei Verlassen der Einrichtung eingezogen.

70. Kritische Einrichtungen werden durch eine unterbrechungsfreie Stromversorgung (USV) oder Generatoren gegen Stromausfälle gesichert, um einen kontinuierlichen Betrieb zu gewährleisten.

71. Kritische Geräte wie USV, Generatoren, Rauchmelder, Feuerlöschsysteme und Zugangskontrollsysteme werden regelmäßig gewartet, und es werden Aufzeichnungen darüber geführt.

72. Zum Schutz vor Elementarschäden sind die Einrichtungen mit feuerfesten Materialien gebaut und mit Brandmeldern, Rauchmeldern, Temperatur- und Überflutungssensoren sowie Feuerlöschern ausgestattet.

73. Es werden sichere Entsorgungsmechanismen für Daten in Papier- und elektronischen Formaten definiert, wobei für Papier Aktenvernichter und für elektronische Medien Methoden wie Bereinigung, Entmagnetisierung oder Vernichtung eingesetzt werden.

74. Eine Richtlinie für einen sauberen Schreibtisch gewährleistet den sicheren Umgang mit Post-it-Zetteln, schriftlichen Dokumenten und Wechselmedien.

75. Die physischen und umgebungsbezogenen Kontrollen werden mindestens einmal jährlich auf ihre Wirksamkeit hin überprüft.

Privatsphäre und Datenschutz

Wenn der Anbieter oder sein Unterauftragsverarbeiter im Auftrag von Alludo oder den Kunden von Alludo personenbezogene Daten verarbeitet, muss er Folgendes sicherstellen:

76. Einhaltung des Datenschutzes und Governance:

76.1. Es werden alle geltenden Datenschutzgesetze eingehalten.

76.2. Es wird ein Rahmen für das Datenschutzmanagement geschaffen, der Folgendes umfasst:

76.3. Datenschutzrichtlinien, -erklärungen, -mitteilungen und -verfahren (die jährlich überprüft werden)

76.4. Datenschutz-Governance und Risikomanagementprozesse

76.5. Einhaltung der rechtlichen und regulatorischen Anforderungen

76.6. Für die personenbezogenen Daten von Alludo werden aktuelle Aufzeichnungen über die Verarbeitungstätigkeiten geführt.

76.7. Es werden geeignete Rollen und Verantwortlichkeiten für den Datenschutz festgelegt und umgesetzt:

76.8. Ernennung eines leitenden Datenschutzbeauftragten (oder einer gleichwertigen Funktion)

76.9. Einrichtung einer speziellen Datenschutz-Funktion

76.10. Bildung eines Ausschusses zur Koordinierung der Aktivitäten zur Einhaltung des Datenschutzes

77. Datenschutz und Sicherheitsmaßnahmen

77.1. Es werden branchenübliche Sicherheitsmaßnahmen (z. B. ISO/IEC 27001:2013, SOC2 usw.) zum Schutz der Informationen von Alludo umgesetzt.

77.2. Für sensible personenbezogene Daten werden zusätzliche Sicherheitsvorkehrungen angewendet (z. B. Verschlüsselung, Pseudonymisierung).

77.3. Es werden Zugangskontrollen durchgesetzt:

77.4. Der Zugang wird nach dem Prinzip der minimalen Berechtigung und dem Need-to-know-Prinzip beschränkt.

77.5. Bei einer Kündigung oder einem Rollenwechsel werden die Zugriffsberechtigungen umgehend aufgehoben.

77.6. Es werden regelmäßige Überprüfungen der Zugriffsberechtigungen durchgeführt.

77.7. Es wird sichergestellt, dass alle Mitarbeiter, die personenbezogene Daten verarbeiten, eine Geheimhaltungsverpflichtung unterzeichnen.

78. Verwaltung der Rechte betroffener Personen:

78.1. Alludo wird bei der Erfüllung seiner Verpflichtungen bezüglich der Rechte betroffener Personen unterstützt.

78.2. Alludo wird innerhalb von zwei Tagen über Anfragen von betroffenen Personen informiert.

78.3. Sofern keine anderslautenden gesetzlichen Bestimmungen bestehen, sind Anfragen ausschließlich auf Anweisung von Alludo zu beantworten.

79. Reaktion auf Vorfälle:

79.1. Alludo muss innerhalb von 24 Stunden über Sicherheitsverletzungen in Bezug auf Alludo-Daten informiert werden.

Maßnahme bei der Vergabe von Unteraufträgen

Der Anbieter muss Folgendes sicherstellen:

80. Es werden jährliche Risikobewertungen für alle Unterauftragsverarbeiter durchgeführt, die an der Handhabung, Verarbeitung oder Speicherung von Alludo-Daten beteiligt sind. Diese Bewertungen müssen die Sicherheitskontrollen, die Datenschutzmaßnahmen, die Einhaltung der einschlägigen Vorschriften und die allgemeine Risikolage des Unterauftragsverarbeiters beurteilen. Die Anbieter müssen diese Bewertungen auf Anfrage belegen, erkannte Risiken umgehend beheben und etwaige Änderungen bei den Unterauftragsverarbeitern oder wichtige Erkenntnisse zeitnah melden. Wir behalten uns das Recht vor, die Ergebnisse der Bewertungen zu überprüfen und erforderlichenfalls zusätzliche Sicherheitsmaßnahmen zu verlangen.

Betriebskontinuitätsmanagement

Der Anbieter muss Folgendes sicherstellen:

81. Es wird eine Richtlinie zum Betriebskontinuitätsmanagement (BCM) geschaffen, die von detaillierten Plänen und Verfahren begleitet wird. Diese Dokumente legen die Geschäftskontinuitätsziele der Organisation dar und werden jährlich überprüft und genehmigt.

82. Es wird ein BCM-Prüfrahmen entwickelt und implementiert, um die Wirksamkeit bestehender Geschäftskontinuitätsstrategien zu bewerten.

83. Mindestens einmal jährlich oder nach wesentlichen organisatorischen Änderungen werden Business-Impact-Analysen (BIA) durchgeführt.

84. Es wird ein Krisenmanagementplan erstellt, der auch spezifische Bestimmungen für die Pandemievorsorge enthält. Dieser Plan stellt eine angemessene Reaktion auf Notfälle sicher und konzentriert sich auf den Schutz von Mitarbeitern, Besuchern, der Umwelt und Ressourcen sowie auf die Aufrechterhaltung wichtiger Geschäftsabläufe.

85. Das Betriebskontinuitätsmanagement-System (BCMS) wird jährlich einem Wirksamkeitstest unterzogen, wobei für jeden Test detaillierte Aufzeichnungen geführt werden.

<Dokumentende>