Technische und organisatorische Sicherheitsmaßnahmen (TOMs) der Infinitas Security GmbH

Gültig ab:
07.07.2026

Inhaltsverzeichnis

Einführung

Sicherheit ist ein wesentlicher Bestandteil der Leistungen der Infinitas Security GmbH („Infinitas“). Diese Übersicht beschreibt ausgewählte technische und organisatorische Maßnahmen, mit denen Infinitas Kundendaten und, soweit einschlägig, kundenseitig bereitgestellte Inhalte vor unbefugtem Zugriff, unbefugter Nutzung, Veränderung, Offenlegung oder Zerstörung schützt.

Die Sicherheitsmaßnahmen von Infinitas orientieren sich an anerkannten Industriestandards sowie an den Anforderungen von ISO/IEC 27001:2022 und ISO/IEC 27002:2022. Infinitas unterhält ein nach ISO/IEC 27001:2022 zertifiziertes Informationssicherheitsmanagementsystem. Diese Übersicht stellt keine vollständige Offenlegung des internen Kontrollrahmens dar. Weitere Details zur Sicherheitsarchitektur und zu relevanten Kontrollen stellt Infinitas im Rahmen von Vertriebs-, Due-Diligence- oder Sicherheitsprüfungen auf Anfrage bereit.

Planung

Infinitas unterhält Richtlinien, Kontrollen und Verfahren, um Sicherheits- und Compliance-Anforderungen frühzeitig in die Planung von Geschäftsabläufen, Systemen und Änderungen einzubeziehen. Dazu gehören insbesondere:

- **Regulatorik:** Infinitas verfolgt relevante gesetzliche, regulatorische und vertragliche Anforderungen im Rahmen des ISMS und berücksichtigt Änderungen bei der Weiterentwicklung von Richtlinien, Verfahren und Kontrollen.
- **Systemdokumentation:** Infinitas dokumentiert relevante Systeme, Geltungsbereiche, Verantwortlichkeiten, Assets und Sicherheitsanforderungen in einem für das Unternehmen angemessenen Umfang.
- **Änderungskommunikation:** Infinitas informiert interne Nutzer und, soweit relevant, Kunden über wesentliche Änderungen an wichtigen Produkten und Services über geeignete Kommunikationswege.
- **Programmreview:** Infinitas überprüft und aktualisiert sein Sicherheitsmanagementprogramm sowie zugehörige Richtlinien und Verfahren mindestens jährlich und anlassbezogen.

Risikomanagement

Infinitas unterhält Richtlinien, Kontrollen und Verfahren für ein risikobasiertes Informationssicherheitsmanagement. Dazu gehören insbesondere:

- **Risikoprozess:** Infinitas identifiziert, bewertet, behandelt und überwacht informationssicherheitsrelevante Risiken, um angemessene und nachvollziehbare Risikomanagement-Entscheidungen zu unterstützen.
- **Policy-Framework:** Infinitas betreibt ein zentrales ISMS-Richtlinienframework, das an ISO/IEC 27001:2022 und weiteren relevanten Anforderungen ausgerichtet ist und der systematischen Risikobehandlung dient.
- **Prüfungen:** Infinitas führt regelmäßige interne Prüfungen und Management Reviews durch und unterzieht das ISMS zudem externen Bewertungen im Rahmen des laufenden Zertifizierungs- und Überwachungsprogramms.

Lieferkettenrisikomanagement

Infinitas unterhält Richtlinien, Kontrollen und Verfahren, um Risiken aus Lieferanten- und Dienstleisterbeziehungen angemessen zu bewerten, zu steuern und fortlaufend zu überwachen. Dazu gehören insbesondere:

- **Lieferantenrahmen:** Infinitas betreibt ein strukturiertes Vorgehen für die Auswahl, Bewertung, Steuerung und regelmäßige Überprüfung von Lieferanten über deren gesamten Lebenszyklus.
- **Prüfprozess:** Neue und bestehende Drittparteien werden risikobasiert einer Sicherheits- und Compliance-Prüfung unterzogen, einschließlich Due Diligence, Vertragsprüfung und fortlaufender Überwachung in angemessenem Umfang.
- **Rollenmodell:** Die Prüfung und Steuerung von Drittparteien erfolgt durch klar zugewiesene Rollen, insbesondere Geschäftsleitung, InfoSec-Funktion und jeweils zuständige fachliche Verantwortliche; externe rechtliche Unterstützung wird bei Bedarf einbezogen.
- **Risikobewertung:** Lieferanten werden vor Onboarding sowie anlassbezogen und in angemessenen Intervallen entsprechend ihrem Risikoprofil neu bewertet, insbesondere bei wesentlichen Leistungs-, Vertrags- oder Risikoveränderungen.
- **Lieferantenregister:** Infinitas führt ein zentrales Register relevanter Lieferanten und dokumentiert dort unter anderem Zuständigkeiten, Leistungsbezug und Risikoeinstufung.
- **Nachweisprüfung:** Soweit relevant und verfügbar, prüft Infinitas geeignete Assurance-Nachweise, Zertifizierungen, Sicherheitsunterlagen und sonstige Informationen zu eingesetzten Dienstleistern regelmäßig.

Awareness und Schulungen

Infinitas unterhält ein formales Set von Richtlinien, Kontrollen und Verfahren für angemessene Schulungen und Security-Awareness-Maßnahmen. Dazu gehören insbesondere:

- **Basis-Schulung:** Mitarbeitende werden im Rahmen des Onboardings mit den für ihre Tätigkeit relevanten Sicherheitsvorgaben vertraut gemacht und absolvieren mindestens jährlich eine Security-Awareness-Schulung; dabei werden für Infinitas relevante Themen der Informationssicherheit sowie einschlägige Datenschutz- und Compliance-Anforderungen adressiert.
- **Rollenbezug:** Für Rollen mit erhöhten Rechten oder besonderer Sicherheitsverantwortung stellt Infinitas rollenbezogene Richtlinien, Verfahren und Arbeitsanweisungen bereit und ergänzt diese bei Bedarf um gezielte, auf die jeweilige Rolle zugeschnittene Einweisungen.
- **Laufende Awareness:** Security-Awareness wird bei Infinitas nicht nur punktuell, sondern regelmäßig und anlassbezogen durch Schulungen, Onboarding-Unterlagen, Richtlinienkommunikation und wiederkehrende Hinweise zu aktuellen Risiken und guten Sicherheitspraktiken gestärkt; dies gilt auch für relevante externe Mitwirkende im ISMS-Geltungsbereich.
- **Pflichtschulung:** Sicherheitsgrundsätze werden durch verpflichtende jährliche Security-Awareness-Schulungen gestärkt; Infinitas betont dabei, dass

Informationssicherheit eine gemeinsame Verantwortung aller Mitarbeitenden und eingebundenen Personen ist.

Personalsicherheit

Infinitas unterhält Richtlinien, Kontrollen und Verfahren, um die Sicherheit von Mitarbeitenden und eingebundenen externen Personen mit Zugriff auf Unternehmens- oder Kundendaten über den gesamten Tätigkeitszyklus hinweg angemessen zu steuern. Dazu gehören insbesondere:

- **Vorabprüfung:** Infinitas prüft vor der Zugriffsvergabe Identität, Qualifikation und Berechtigung der jeweiligen Person und kann für besonders sicherheitskritische Rollen weitergehende Prüfungen vorsehen.
- **Onboarding:** Das Onboarding bei Infinitas umfasst den Abschluss von Arbeits- oder Dienstleistungsverträgen, Vertraulichkeitsverpflichtungen, Sicherheitsschulungen sowie die Bestätigung einschlägiger Sicherheitsvorgaben und rollenbezogener Pflichten.
- **Policy-Rahmen:** Personalbezogene Sicherheitsanforderungen sind bei Infinitas in einschlägigen Richtlinien und Verfahren geregelt und werden im Rahmen des ISMS mindestens jährlich sowie anlassbezogen überprüft.
- **Rollenwechsel:** Rollenwechsel und Austritte unterliegen dokumentierten Joiner-Mover-Leaver-Prozessen, einschließlich Neubewertung von Zugriffsrechten, zeitnaher Entziehung nicht mehr erforderlicher Zugriffe, Offboarding-Checklisten und erneuter Freigabe bei späterer Wiedervergabe von Zugriffen.
- **Disziplinarprozess:** Infinitas betreibt ein dokumentiertes Disziplinarverfahren, um Verstöße gegen Sicherheitsvorgaben angemessen, nachvollziehbar und verhältnismäßig zu bewerten und zu behandeln.

Prüfung, Autorisierung und Monitoring

Infinitas unterhält formale Richtlinien, Kontrollen und Verfahren, um die Wirksamkeit seines ISMS, seiner Sicherheitsmaßnahmen sowie seiner Entwicklungs- und Cloud-Umgebungen regelmäßig zu prüfen, Abweichungen systematisch nachzuverfolgen und Risiken frühzeitig zu erkennen. Dazu gehören insbesondere:

- **Auditrahmen:** Infinitas definiert verbindliche Vorgaben für Audits, Reviews und Wirksamkeitsprüfungen im Rahmen seines ISMS und überprüft diese mindestens jährlich sowie anlassbezogen bei wesentlichen Änderungen.
- **Policy-Framework:** Infinitas betreibt ein zentrales ISMS-Richtlinienframework mit thematisch gegliederten Richtlinien und Verfahren; diese werden versioniert verwaltet, regelmäßig überprüft und durch die zuständige Leitung von Infinitas freigegeben.
- **Auditsteuerung:** Audits und vergleichbare Prüfungen werden geplant, risikobasiert priorisiert, anhand definierter Kontrollziele durchgeführt, dokumentiert bewertet und mit konkreten Maßnahmen, Fristen und Verantwortlichkeiten nachverfolgt; frühere Audit-, Review- und Vorfallergebnisse werden dabei berücksichtigt.

- **Externe Audits:** Infinitas führt interne Audits, Management Reviews und weitere Wirksamkeitsprüfungen durch, berücksichtigt externe Assurance-Nachweise relevanter Dienstleister und unterhält ein nach ISO/IEC 27001:2022 zertifiziertes ISMS. Das ISMS sowie die Angemessenheit und Wirksamkeit relevanter Kontrollen und Prozesse werden im Rahmen externer Zertifizierungs- und Überwachungsaudits unabhängig bewertet.
- **Compliancеprüfung:** Infinitas überprüft fortlaufend die Konformität mit relevanten gesetzlichen, regulatorischen und vertraglichen Anforderungen sowie mit den Anforderungen von ISO/IEC 27001:2022 im Rahmen des zertifizierten ISMS und des laufenden Audit- und Verbesserungsprogramms.
- **Abweichungsmanagement:** Festgestellte Abweichungen und Nichtkonformitäten werden systematisch erfasst, nach Ursache bewertet, mit Korrekturmaßnahmen versehen, Verantwortlichen zugewiesen und bis zum Abschluss nachverfolgt.
- **Schwachstellenscans:** Infinitas setzt im SSDLC und im laufenden Betrieb wiederkehrende und weitgehend automatisierte Sicherheitstests ein, insbesondere Secrets-Scans, SAST-, SCA- und DAST-Prüfungen; erkannte Schwachstellen werden nach Schweregrad und Kritikalität priorisiert und innerhalb definierter Prozesse behoben oder formal risikobezogen behandelt.
- **Sicherheitsbewertungen:** Sicherheits- und Schwachstellenbewertungen für relevante Cloud-Produkte und Prozesse sind in Projektinitiierung, SSDLC, wiederkehrenden Betriebsaktivitäten und jährlichen Prüfungen verankert; datenschutzbezogene Risiken werden insbesondere bei neuen oder geänderten Verarbeitungen sowie bei GDPR-relevanten Projekten bewertet und dokumentiert.

Identifizierung und Authentifizierung

Infinitas unterhält Richtlinien, Kontrollen und Verfahren, um Identitäten eindeutig zuzuordnen und Zugriffe angemessen zu authentifizieren. Dazu gehören insbesondere:

- **Identitätssystem:** Identitäten werden zentral verwaltet und Zugänge eindeutig einer berechtigten Person zugeordnet.
- **SSO:** Single Sign-on wird für geeignete Anwendungen risikobasiert eingesetzt und, soweit technisch und wirtschaftlich angemessen, weiter ausgebaut.
- **MFA-Absicherung:** Für relevante Zugriffe auf Unternehmens- und Cloud-Dienste setzt Infinitas Mehrfaktor-Authentifizierung als Standard ein; zusätzliche Zugriffsbedingungen werden zentral gesteuert.
- **Passwortregeln:** Infinitas definiert verbindliche Anforderungen für den sicheren Umgang mit Passwörtern und Anmeldedaten, insbesondere hinsichtlich Vertraulichkeit, Nutzung und Aufbewahrung.
- **Geheimnisschutz:** Zugangsdaten, Tokens, Schlüssel und sonstige Geheimnisse werden durch geeignete technische und organisatorische Maßnahmen geschützt und nicht unkontrolliert in Code oder ungesicherten Speichern abgelegt.
- **Freigaben und Reviews:** Benutzerkonten und Zugriffsrechte unterliegen dokumentierten Freigaben, regelmäßigen Überprüfungen und anlassbezogenen Anpassungen im Rahmen des Joiner-Mover-Leaver-Prozesses.

Zugriffskontrolle

Infinitas unterhält ein angemessenes Set dokumentierter Richtlinien, Kontrollen und Verfahren für eine angemessene Zugriffskontrolle bei der Verarbeitung von Kundendaten und Kundenmaterialien. Dazu gehören insbesondere:

- **Zugriffsrichtlinie:** Infinitas betreibt eine formale Richtlinie und zugehörige Verfahren für das Zugriffsmanagement, die Zugriffsstandards, Zuständigkeiten, Genehmigungen sowie die Grundsätze für die Anlage, Änderung und Entziehung von Benutzerzugängen regeln.
- **Schutzbedarf:** Infinitas ordnet Systeme, Daten und Zugriffsarten risikobasiert nach Schutzbedarf und Kritikalität ein und definiert darauf aufbauend verstärkte Anforderungen für privilegierte oder besonders schutzbedürftige Zugriffe, insbesondere die verpflichtende Nutzung von Mehrfaktor-Authentifizierung.
- **Rollenbezug:** Zugriffe auf Systeme, Anwendungen und Infrastruktur von Infinitas werden rollenbasiert und nach dem Least-Privilege-Prinzip vergeben, sodass nur autorisierte Personen Zugriff auf Entwicklungs-, Build- und produktbezogene Quellcode-Umgebungen erhalten.
- **Need-to-know:** Infinitas wendet strikte rollenbasierte Zugriffsrechte für Mitarbeitende, Freelancer und sonstige berechtigte Personen an, sodass Zugriff auf Kundendaten ausschließlich nach dem Need-to-know-Prinzip und nur im für die jeweilige Aufgabe erforderlichen Umfang gewährt wird.
- **Supportzugriffe:** Zugriff auf Kundendaten durch Infinitas erfolgt nur, soweit dies für Betrieb, Support, Sicherheit oder vertraglich vereinbarte Leistungen erforderlich ist. Solche Zugriffe werden auf berechtigte Rollen beschränkt.
- **Funktionstrennung:** Infinitas setzt Funktionstrennung mit besonderem Fokus auf den Entwicklungsprozess und den SSDLC um, insbesondere durch dokumentierte Freigabe- und Workflow-Kontrollen, rollenbezogene Berechtigungen in Entwicklungs- und Quellcode-Umgebungen, Vier-Augen-Prinzipien bei codebezogenen Änderungen.
- **Freigabeprozess:** Benutzerkonten und Zugriffsrechte werden vor der Freischaltung auf Daten, Anwendungen, Infrastruktur oder Netzwerkkomponenten unter Berücksichtigung von Rolle, Schutzbedarf und Systemverantwortung genehmigt; bestehende Zugriffe werden regelmäßig und anlassbezogen überprüft.
- **Schutzmechanismen:** Infinitas setzt abhängig von Schutzbedarf und Einsatzszenario technische Zugriffsschutzmaßnahmen ein, insbesondere Mehrfaktor-Authentifizierung und Conditional Access.
- **Gerätesteuerung:** Infinitas betreibt eine zentral verwaltete Endpoint- und Mobile-Sicherheitssteuerung, einschließlich definierter automatischer Sperrzeiten für Unternehmensgeräte, Compliance-Prüfungen für verwaltete Endgeräte sowie MAM-Schutzmechanismen für zugelassene BYOD-Szenarien.
- **Kontenpflege:** Infinitas identifiziert und entfernt nicht mehr benötigte, veraltete oder inaktive Zugänge im Rahmen von Joiner-Mover-Leaver-Prozessen, anlassbezogenen Prüfungen und regelmäßigen Reviews, einschließlich zeitnaher Entziehung von Zugriffen sowie automatisierter Entzüge oder Selektivlöschungen dort, wo die eingesetzten Plattformen dies unterstützen.

Konfigurationsmanagement

Infinitas unterhält formale Richtlinien, Kontrollen und Verfahren, um Konfigurationen, Änderungen und technische Baselines kontrolliert zu steuern, unautorisierte Änderungen zu erschweren und die Nachvollziehbarkeit über den gesamten Lebenszyklus von Systemen, Anwendungen, Endgeräten und Cloud-Ressourcen sicherzustellen. Dazu gehören insbesondere:

- **Änderungssteuerung:** Infinitas steuert Änderungen an produktionsrelevanter Software, Build- und Deployment-Prozessen sowie sicherheitsrelevanten Konfigurationen über dokumentierte Verfahren. Sicherheitsanforderungen und Risiken werden bereits in Planung und Design erfasst, produktive Änderungen werden dokumentiert, geprüft und freigegeben.
- **Policy-Framework:** Infinitas betreibt ein zentrales ISMS-Richtlinienframework mit thematisch gegliederten Richtlinien und Verfahren, die versioniert verwaltet, mindestens jährlich überprüft und von der zuständigen Leitung freigegeben werden.
- **Freigabestandards:** Infinitas definiert Baselines und Freigabestandards für Änderungen. Vor der Umsetzung müssen je nach Änderung dokumentierte Sicherheits- und Testanforderungen erfüllt sein.
- **Peer Review:** Produktionsrelevante Code- und Infrastrukturänderungen unterliegen dem Vier-Augen-Prinzip. Pull Requests erfordern mindestens eine unabhängige Peer-Review-Freigabe sowie erfolgreiche Security-Gates und Tests, soweit diese für den jeweiligen Änderungstyp anwendbar sind, bevor eine Promotion in höhere Umgebungen oder ein Produktiv-Deployment erfolgen kann.
- **Notfalländerungen:** Infinitas erlaubt Break-Glass-Änderungen nur zum Schutz der Serviceverfügbarkeit oder zur Behebung kritischer Sicherheits- oder Betriebsrisiken. Solche Änderungen werden im Nachgang zeitnah retrospektiv geprüft, dokumentiert und genehmigt.
- **Asset-Inventar:** Infinitas erfasst und verfolgt physische und logische Assets zentral, einschließlich Eigentümer, Klassifikation, Abhängigkeiten, Status und eindeutiger Kennzeichnungen; die Vollständigkeit und Eigentümerschaft werden regelmäßig überprüft.
- **Betriebsüberwachung:** Infinitas überwacht Gesundheitszustand, Auslastung, Kapazität und Verfügbarkeit relevanter Assets und Cloud-Produkte mit nativen Monitoring- und Alerting-Funktionen der eingesetzten Plattformen; Kapazitätsprüfungen erfolgen regelmäßig, wobei vorhandene Autoscaling- und Telemetrie-Funktionen genutzt werden.

System- und Servicebeschaffung

Infinitas unterhält Richtlinien, Kontrollen und Verfahren für die sichere Entwicklung, Änderung und Bereitstellung von Systemen und Services. Dazu gehören insbesondere:

- **SSDLC:** Infinitas setzt einen dokumentierten Secure Software Development Life Cycle ein, in dem sicherheitsrelevante Anforderungen, Prüfungen und Nachweise von der Planung bis zum Betrieb verankert sind.

- **Bereitstellung:** Infinitas nutzt standardisierte und weitgehend automatisierte Prozesse für Anwendungs- und Konfigurationsänderungen; produktive Änderungen unterliegen zusätzlichen Freigaben.
- **Reviews und Tests:** Infinitas verlangt für relevante Änderungen einen definierten Entwicklungsprozess mit Peer Review und verpflichtenden automatisierten Prüfungen vor Zusammenführung und Bereitstellung.
- **Funktionstrennung:** Infinitas setzt für Änderungen definierte Rollen, Freigaben und Vier-Augen-Prinzipien ein. Wo eine vollständige organisatorische Trennung nicht zweckmäßig oder nicht möglich ist, werden kompensierende Kontrollen wie Peer Reviews, technische Freigaben, Protokollierung und nachgelagerte Prüfung angewendet.
- **Notfalländerungen:** Infinitas unterhält ein dokumentiertes Verfahren für Notfalländerungen einschließlich Break-Glass-Szenarien, mit nachgelagerter Prüfung und Freigabe.
- **Änderungsschutz:** Infinitas schützt Quellcode- und Deployment-Systeme durch technische und organisatorische Kontrollen, um unautorisierte Änderungen zu verhindern oder zu erschweren.
- **Änderungsnachweise:** Relevante Code-, Infrastruktur- und Konfigurationsänderungen werden nachvollziehbar dokumentiert; definierte Prüf- und Freigabeschritte werden technisch erzwungen.
- **Dokumentation:** Infinitas pflegt für relevante Cloud- und Software-Services eine angemessene technische und betriebliche Dokumentation, einschließlich sicherheitsrelevanter Vorgaben zur Nutzung und Konfiguration.
- **Abhängigkeitsmanagement:** Infinitas überprüft den Codebestand sowie Drittanbieter- und Open-Source-Abhängigkeiten regelmäßig mit geeigneten Sicherheitsprüfungen und steuert erforderliche Updates risikobasiert.

System- und Kommunikationsschutz

Infinitas unterhält Richtlinien, Kontrollen und Verfahren zum Schutz von Systemen, Netzwerken, Endgeräten und Datenübertragungen. Dazu gehören insbesondere:

- **Kryptografie:** Infinitas schützt sensible Daten bei Speicherung und Übertragung durch geeignete kryptografische Verfahren nach dem Stand der Technik.
- **Verschlüsselung:** Infinitas setzt für relevante Cloud- und Anwendungskomponenten Verschlüsselung für Daten im Ruhezustand und bei der Übertragung ein, insbesondere mittels TLS 1.2+ und starker, branchenüblicher Verfahren.
- **Sichere Informationsübertragung:** Infinitas nutzt zugelassene Kommunikations- und Transferkanäle mit angemessenen Schutzmaßnahmen, insbesondere Verschlüsselung während der Übertragung, Zugriffsbeschränkungen und risikobasierte Freigaben für externe Weitergaben.
- **Klassifizierung und DLP:** Infinitas klassifiziert Informationen nach Schutzbedarf und setzt, soweit technisch verfügbar und angemessen, ergänzende Data-Loss-Prevention- und Schutzmechanismen für relevante Cloud- und Kommunikationsdienste ein.

- **Umgebungstrennung:** Infinitas trennt Entwicklungs-, Test- und Produktivumgebungen logisch und beschränkt Verbindungen zwischen diesen Umgebungen auf das erforderliche Maß.
- **Endpunktschutz:** Infinitas verwaltet Unternehmensgeräte zentral und setzt verbindliche Baselines für Patches, Passwort- beziehungsweise Re-Authentifizierungsschutz, Bildschirmsperren und Laufwerksverschlüsselung um.
- **Gerätevertrauen:** Zugriffe auf Unternehmensressourcen werden risikobasiert über Geräte-, Identitäts- und App-Schutzkontrollen beschränkt; für freigegebene BYOD- und externe Zugriffsszenarien gelten definierte Schutzmaßnahmen.
- **Firewallschutz:** Infinitas setzt in seinen Cloud-Umgebungen Firewalls, Netzwerkregeln und vorgeschaltete Schutzmechanismen ein, um Zugriffe auf das erforderliche Maß zu begrenzen.
- **Netzwerkhärtung:** Infinitas nutzt Maßnahmen wie Systemhärtung, Netzwerksegmentierung, Endpoint-Schutz und weitere geeignete Kontrollen zum Schutz vor unautorisierten Zugriffen und Sicherheitsereignissen.
- **Datentrennung:** Infinitas setzt geeignete logische Trennungs-, Mandantenisolations- und Zugriffskontrollen ein, um Kundendaten mandantenbezogen voneinander sowie von anderen Datenbeständen getrennt zu halten.

Medienschutz

Infinitas unterhält Richtlinien, Kontrollen und Verfahren zum Schutz von Datenträgern, Endgeräten und sonstigen Medien mit Unternehmens- und Kundendaten. Dazu gehören insbesondere:

- **Physische Sicherheit und Providerbetrieb:** Infinitas betreibt keine eigenen Rechenzentren für die SaaS-Plattform, sondern nutzt ausgewählte Cloud- und SaaS-Anbieter, insbesondere Microsoft Azure. Physische Sicherheitsmaßnahmen für die zugrunde liegende Rechenzentrumsinfrastruktur werden im Rahmen des Shared-Responsibility-Modells durch die jeweiligen Anbieter erbracht und risikobasiert über verfügbare Assurance-Nachweise berücksichtigt.
- **Medienentsorgung:** Infinitas verlangt für eigene Datenträger und Endgeräte eine sichere Löschung oder kryptografische Bereinigung vor Wiederverwendung, Reparatur oder Entsorgung; bei ausgelagerten Cloud-Ressourcen stützt sich Infinitas auf die dokumentierten Lösch- und Entsorgungsprozesse des jeweiligen Anbieters.
- **Verschlüsselung:** Infinitas schützt relevante Daten und Endgeräte durch angemessene Verschlüsselungsmaßnahmen nach dem Stand der Technik, insbesondere für Daten im Ruhezustand und bei der Übertragung sowie für verwaltete Unternehmensgeräte.
- **BYOD-Schutz:** Infinitas erlaubt zugelassene BYOD-Szenarien nur unter definierten Sicherheitsvorgaben, insbesondere mit Freigabeprozess, App-Schutz, Zugriffsbeschränkungen und Schutzmaßnahmen für nicht konforme oder nicht geschützte Zugriffsszenarien.
- **Clear desk:** Infinitas verlangt für unbeaufsichtigte Arbeitsplätze Clear-desk- und Clear-screen-Maßnahmen, damit vertrauliche Informationen und Geräte nicht ungeschützt einsehbar oder zugänglich sind.

System- und Informationsintegrität

Infinitas unterhält Richtlinien, Kontrollen und Verfahren, um die Integrität von Systemen und Informationen zu schützen, unzulässige Veränderungen zu erkennen und Daten über ihren gesamten Lebenszyklus angemessen zu behandeln.

- **Testdaten:** Infinitas nutzt in Nicht-Produktivumgebungen grundsätzlich synthetische oder anonymisierte Testdaten.
- **Datenschutz und Datenminimierung:** Infinitas verarbeitet personenbezogene Daten nach dem Grundsatz der Zweckbindung und Datenminimierung. Neue oder wesentlich geänderte Verarbeitungen werden risikobasiert auf Datenschutz- und Informationssicherheitsanforderungen geprüft.
- **Datenlöschung und Aufbewahrung:** Infinitas definiert angemessene Aufbewahrungs- und Löschprozesse für Unternehmens- und Kundendaten. Löschungen erfolgen nach vertraglichen, gesetzlichen und technischen Anforderungen sowie nach den Möglichkeiten der eingesetzten Plattformen.
- **Protokollschutz:** Infinitas protokolliert sicherheitsrelevante Ereignisse über die vorgesehenen Plattformfunktionen, schützt Protokolle vor unbefugtem Zugriff und unzulässiger Veränderung und bewahrt sie für einen angemessenen Zeitraum auf.
- **Zugriffsprotokollierung:** Soweit technisch verfügbar, protokolliert Infinitas relevante Benutzer-, Administrations- und Zugriffsvorgänge in produktrelevanten Systemen, um Nachvollziehbarkeit, Untersuchung und Auditierbarkeit zu unterstützen.
- **Malwareschutz:** Infinitas setzt auf verwalteten Systemen geeignete Schutzmaßnahmen gegen Malware ein und berücksichtigt entsprechende Sicherheitswarnungen der eingesetzten Plattformen.
- **Identitätsbindung:** Infinitas verwendet eindeutig zugeordnete Identitäten für Benutzer- und Dienstkonten und beschränkt Zugriffe durch rollenbasierte sowie identitätsgebundene Kontrollen auf das erforderliche Maß.
- **Umgebungstrennung:** Infinitas trennt Produktiv- und Nicht-Produktivumgebungen logisch und organisatorisch, um unbeabsichtigte Vermischung, unzulässige Zugriffe und Integritätsrisiken zu reduzieren.
- **Sandbox-Schutz:** Für Entwicklungs-, Test- und Fehleranalyseumgebungen gelten definierte Schutzvorgaben, insbesondere zur Datenminimierung, Zugriffsbeschränkung sowie zum sicheren Umgang mit Artefakten und sensiblen Inhalten.

Audit und Nachvollziehbarkeit

Infinitas unterhält formale Richtlinien, Kontrollen und Verfahren, um sicherheitsrelevante Aktivitäten nachvollziehbar zu protokollieren, Auffälligkeiten zu erkennen und eine belastbare Nachvollziehbarkeit für Untersuchungen, Reviews und Audit-Zwecke sicherzustellen. Dazu gehören insbesondere:

- **Loggingstandard:** Infinitas definiert verbindliche Anforderungen an Protokollierung und Monitoring im Rahmen seines ISMS-Richtlinienrahmens,

einschließlich Vorgaben zu relevanten Ereignistypen, Schutz der Protokolldaten, Aufbewahrung, Überprüfung und Eskalation.

- **Logspeicherung:** Relevante System-, Sicherheits-, Identitäts- und Anwendungsprotokolle werden soweit technisch verfügbar automatisiert an die vorgesehenen, verwalteten Logging-Funktionen der eingesetzten Cloud- und SaaS-Plattformen übermittelt und dort geschützt gespeichert; der Zugriff auf Rohprotokolle ist auf eng definierte berechtigte Rollen beschränkt.
- **Anomalieerkennung:** Infinitas überwacht sicherheitsrelevante Protokolle, Warnmeldungen und Audit-Ereignisse, um ungewöhnliche Aktivitäten zu erkennen; für die Sichtung, Bewertung und Bearbeitung von Auffälligkeiten bestehen festgelegte Review- und Eskalationsprozesse.
- **Umfangspflege:** Der Umfang der Protokollierung wird bei neuen Funktionen, Systemänderungen, neuen kritischen Assets oder veränderten Risikolagen überprüft und bei Bedarf angepasst, damit neue Ereignistypen und sicherheitsrelevante Änderungen angemessen erfasst werden.
- **Zeitsynchronisation:** Infinitas stellt sicher, dass Systeme eine automatische Zeitsynchronisation mit vertrauenswürdigen Zeitquellen nutzen, insbesondere über Betriebssystem- oder Cloud-Zeitdienste wie die von Microsoft Azure bereitgestellten Mechanismen, damit Zeitstempel konsistent und forensisch belastbar bleiben.

Notfallplanung

Infinitas unterhält formale Richtlinien, Kontrollen und Verfahren, um auf Störungen, Sicherheitsvorfälle und Ausfälle vorbereitet zu sein, Wiederherstellung planbar zu machen und die Fortführung kritischer Prozesse in einem angemessenen Rahmen sicherzustellen. Dazu gehören insbesondere:

- **Betriebsgrundlage:** Infinitas stützt die Leistungserbringung auf qualifizierte Mitarbeitende, definierte Zuständigkeiten sowie geeignete cloudbasierte Betriebs- und Kommunikationsplattformen.
- **Wiederanlaufplanung:** Infinitas unterhält dokumentierte Vorgaben und Playbooks für Incident Response, Business Continuity, Backup und Wiederherstellung; Wiederanlauf- und Wiederherstellungsziele werden für relevante Assets berücksichtigt.
- **Fortführung:** Infinitas setzt Maßnahmen um, um den Zugriff auf kritische Daten und Systeme im Störungsfall geordnet wiederherstellen und die Nutzung soweit erforderlich fortführen zu können.
- **Cloudbasierte Resilienz:** Infinitas nutzt eine cloudbasierte Architektur mit geeigneten Resilienz- und Wiederherstellungsfunktionen, soweit dies für den jeweiligen Service, Schutzbedarf und Wiederherstellungszweck erforderlich ist.
- **Resilienzkontrollen:** Infinitas stärkt die Betriebsresilienz insbesondere durch regelmäßige Datensicherungen, Wiederherstellungsverfahren und weitere technische sowie organisatorische Schutzmaßnahmen.
- **Vorfallreaktion:** Infinitas betreibt dokumentierte Verfahren zur Reaktion auf Cybersecurity-Ereignisse, um Auswirkungen zu begrenzen, Wiederherstellung zu unterstützen und den Geschäftsbetrieb soweit möglich aufrechtzuerhalten.

- **Kapazitätsmanagement:** Infinitas überwacht Verfügbarkeit, Zustand und Kapazität relevanter Systeme und Services und trifft bei Bedarf geeignete Anpassungs- und Schutzmaßnahmen.
- **Backupschutz:** Infinitas schützt Backups durch angemessene technische und organisatorische Maßnahmen, insbesondere hinsichtlich Vertraulichkeit, Integrität, Verfügbarkeit und Wiederherstellbarkeit.
- **Wiederherstellungstests:** Infinitas überprüft Wiederherstellungsfähigkeiten risikobasiert durch geeignete Tests, Reviews oder technische Nachweise, um die praktische Nutzbarkeit relevanter Backup- und Recovery-Maßnahmen zu bestätigen.

Umgang mit Sicherheitsvorfällen

Infinitas unterhält Richtlinien, Kontrollen und Verfahren, um Sicherheitsvorfälle vorbereitet, strukturiert und nachvollziehbar zu behandeln. Dazu gehören insbesondere:

- **Vorfallplanung:** Infinitas betreibt dokumentierte Incident-Response-Vorgaben und Playbooks für Vorbereitung, Erkennung, Bewertung, Eindämmung, Beseitigung, Wiederherstellung, Beweissicherung und Nachbereitung unter Berücksichtigung datenschutzrechtlicher und sonstiger anwendbarer Anforderungen.
- **Rollenmodell:** Sicherheitsvorfälle werden bei Infinitas durch klar benannte Rollen und Eskalationswege bearbeitet. Dabei arbeiten insbesondere InfoSec-Verantwortung, Geschäftsleitung und betroffene Systemverantwortliche koordiniert zusammen; Triage und Eskalation folgen einem definierten Vorgehen.
- **Übungen und Tests:** Infinitas überprüft seine Reaktionsfähigkeit regelmäßig durch ausgewählte Tests und Übungen, um die Wirksamkeit des Vorfallmanagements fortlaufend zu verbessern.
- **Planpflege:** Incident-Response-Richtlinien und zugehörige Playbooks werden regelmäßig sowie anlassbezogen nach wesentlichen Änderungen oder Vorfällen überprüft und aktualisiert.
- **Lessons Learned:** Für relevante, schwerwiegende oder wiederkehrende Sicherheitsvorfälle sieht Infinitas strukturierte Nachbereitungen mit Ursachenanalyse, Maßnahmenableitung und Nachverfolgung vor, um systematische Verbesserungen umzusetzen.
- **Prozessverankerung:** Verfahren zur Behandlung von Sicherheitsvorfällen sind in relevante Betriebs-, Wiederherstellungs- und Kommunikationsprozesse eingebettet, um Ausfallzeiten und Sicherheitsrisiken zu begrenzen.
- **Kundeninformation:** Infinitas informiert betroffene Kunden über relevante Sicherheitsvorfälle ohne unangemessene Verzögerung nach Maßgabe vertraglicher und gesetzlicher Anforderungen und unterstützt, soweit erforderlich, mit den dafür notwendigen Informationen.
- **Externe Unterstützung:** Infinitas kann bei relevanten Sicherheitsvorfällen externe fachliche, rechtliche, forensische oder versicherungsbezogene Unterstützung einbeziehen, soweit dies für Bewertung, Eindämmung, Wiederherstellung oder Kommunikation erforderlich ist.