Liste der technischen und organisatorischen Maßnahmen CTO Balzuweit GmbH

Stand: 20.08.2026

Angaben zum Verantwortlichen

Name und Kontaktdaten natürliche Person/juristische Person/Behörde/Einrichtung etc.

Name	CTO Balzuweit GmbH
Unternehmensvertreter	Markus Balzuweit
Straße	Lautlinger Weg 3
Postleitzahl	70567
Ort	Stuttgart
Land	Deutschland
Telefon	+49 711 718639-0
E-Mail-Adresse	datenschutz@cto.de

Angaben zur Person des Datenschutzbeauftragten

extern mit Anschrift / sofern gem. Artikel 37 DS-GVO benannt

Name	DataGAP GmbH
Straße	Bessemerstr. 82, 10. OG Süd
Postleitzahl	12103
Ort	Berlin
Land	Deutschland
Telefon	030 / 577 10 513
E-Mail-Adresse	team@datagap.de

Inhaltsverzeichnis

1. Auftragskontrolle (organisatorisch) 3
2. Datenschutz-Management (organisatorisch) 4
3. Datenschutz-Management (technisch) 4
4. Datenschutzfreundliche Voreinstellungen (technisch) 5
5. Eingabekontrolle (organisatorisch) 5
6. Incident-Response-Management (organisatorisch) 5
7. Incident-Response-Management (technisch) 6
8. Transport- und Weitergabekontrolle (organisatorisch) 7
9. Transport- und Weitergabekontrolle (technisch) 7
10. Trennungskontrolle (organisatorisch) 8
11. Trennungskontrolle (technisch) 8
12. Verfügbarkeitskontrolle (organisatorisch) 8
13. Verfügbarkeitskontrolle (technisch) 9
14. Zugangskontrolle (organisatorisch) 10
15. Zugangskontrolle (technisch) 11
16. Zugriffskontrolle/Pseudonymisierung (organisatorisch) 13
17. Zugriffskontrolle/Pseudonymisierung (technisch) 14
18. Zutrittskontrolle (organisatorisch) 15
19. Zutrittskontrolle (technisch) 16

1. Auftragskontrolle (organisatorisch)

   a. **Auftragsverarbeitungsvertrag:** Bevor die CTO Balzuweit GmbH personenbezogene Daten für einen Auftraggeber verarbeitet, wird grundsätzlich ein Auftragsverarbeitungsvertrag (AVV) nach Art. 28 Abs. 3 DSGVO abgeschlossen. Bei Verarbeitungen außerhalb der EU bzw. des EWR kommen zusätzlich die EU-Standardvertragsklauseln der Europäischen Kommission zum Einsatz. Der AVV regelt insbesondere Gegenstand, Dauer, Art und Zweck der Verarbeitung sowie die Kategorien betroffener Personen und wird vor Beginn der Verarbeitung mit dem Auftraggeber final abgestimmt. Änderungen der Verarbeitung werden über ergänzende Weisungen bzw. eine Anpassung der Vertragsanlagen nachgehalten.

   b. **Sorgfältige Auswahl von Unterauftragnehmern:** Setzt CTO ihrerseits Unterauftragnehmer zur Erbringung von Leistungen ein, erfolgt deren Auswahl unter besonderer Berücksichtigung von Datenschutz und Datensicherheit. Vor Beauftragung wird geprüft, ob der jeweilige Dienstleister ein angemessenes Schutzniveau sowie ausreichende technische und organisatorische Maßnahmen nachweisen kann. Bevorzugt werden Anbieter mit anerkannten Zertifizierungen, etwa nach ISO/IEC 27001, sowie mit Verarbeitungsstandorten innerhalb der EU bzw. des EWR. Die Eignung wird nicht nur einmalig zu Vertragsbeginn, sondern in regelmäßigen Abständen erneut bewertet.

   c. **Prüfung der Sicherheitsmaßnahmen von Unterauftragnehmern:** Vor dem Einsatz eines Unterauftragnehmers lässt sich CTO dessen technische und organisatorische Maßnahmen nachweisen, beispielsweise durch Zertifikate, Auditberichte oder eigene TOM-Dokumente des Dienstleisters. Diese Nachweise werden geprüft und für die Dauer der Zusammenarbeit dokumentiert abgelegt. Bei wesentlichen Änderungen der Sicherheitsmaßnahmen eines Unterauftragnehmers wird die Dokumentation aktualisiert und erneut bewertet. Auf Anfrage können entsprechende Nachweise im Rahmen vertraglich vereinbarter Kontrollrechte an Auftraggeber weitergegeben werden.

   d. **Dokumentierte Weisungen:** Weisungen der CTO Balzuweit GmbH an von ihr eingesetzte Unterauftragnehmer erfolgen grundsätzlich schriftlich oder in Textform, etwa per E-Mail oder über ein Ticketsystem. Dies stellt sicher, dass Inhalt und Umfang der beauftragten Verarbeitung jederzeit nachvollziehbar sind. Ausnahmsweise mündlich erteilte Weisungen werden unverzüglich in Textform nachgehalten und bestätigt. Die dokumentierten Weisungen sind Bestandteil der jeweiligen Auftragsakte und stehen im Bedarfsfall für Nachweiszwecke zur Verfügung.

   e. **Verpflichtung auf das Datengeheimnis:** CTO stellt vertraglich sicher, dass auch die Mitarbeitenden eingesetzter Unterauftragnehmer auf die Vertraulichkeit personenbezogener Daten verpflichtet werden. Diese Verpflichtung umfasst insbesondere das Datengeheimnis gemäß Art. 28 Abs. 3 lit. b DSGVO sowie ergänzende vertragliche Vertraulichkeitsregelungen. Der Nachweis der Verpflichtung kann von CTO im Rahmen der Kontrollrechte gegenüber dem Unterauftragnehmer angefordert werden. Damit wird sichergestellt, dass die Vertraulichkeit über die gesamte Verarbeitungskette hinweg gewahrt bleibt.

   f. **Datenschutzbeauftragter beim Unterauftragnehmer:** Sofern für einen von CTO eingesetzten Unterauftragnehmer nach Art. 37 DSGVO eine Pflicht zur Benennung eines Datenschutzbeauftragten besteht, wird dies vertraglich vorausgesetzt und im Rahmen der Beauftragung überprüft. Der Unterauftragnehmer hat CTO auf Anfrage Name und Kontaktdaten des benannten Datenschutzbeauftragten mitzuteilen. Ein Wechsel ist unverzüglich anzuzeigen. Dadurch stellt CTO sicher, dass auch bei weiteren Gliedern der Verarbeitungskette ein datenschutzrechtlicher Ansprechpartner benannt ist.

   g. **Kontrollrechte gegenüber Unterauftragnehmern:** In den Verträgen mit eingesetzten Unterauftragnehmern vereinbart CTO wirksame Kontrollrechte, die es erlauben, die Einhaltung der vereinbarten technischen und organisatorischen Maßnahmen zu überprüfen. Dies umfasst je nach Vereinbarung Auskunftsrechte, die Vorlage von Nachweisen und

Zertifikaten sowie in begründeten Fällen Vor-Ort-Kontrollen. Die Kontrollrechte werden so ausgestaltet, dass sie auch von Aufsichtsbehörden oder im Auftrag von CTO-Kunden im erforderlichen Umfang genutzt werden können. Damit stellt CTO die Nachvollziehbarkeit der Datenverarbeitung entlang der gesamten Auftragskette sicher.

2. Datenschutz-Management (organisatorisch)

   a. **Schulung und Verpflichtung der Mitarbeitenden:** Alle Mitarbeitenden der CTO Balzuweit GmbH werden im Rahmen des Onboardings auf die Vertraulichkeit personenbezogener Daten sowie das Datengeheimnis verpflichtet. Ergänzend erhalten neue Mitarbeitende eine Einführung in die grundlegenden Datenschutz- und Informationssicherheitsanforderungen des Unternehmens. Die Verpflichtungserklärung wird dokumentiert und in der Personalakte hinterlegt. Sie gilt fort über das Ende des Beschäftigungsverhältnisses hinaus.

   b. **Regelmäßige Sensibilisierung:** Über die initiale Schulung hinaus werden Mitarbeitende der CTO Balzuweit GmbH mindestens jährlich zu Themen des Datenschutzes und der Informationssicherheit sensibilisiert. Die Inhalte werden fortlaufend an aktuelle Bedrohungslagen angepasst, etwa zu Phishing, Social Engineering oder dem sicheren Umgang mit mobilen Endgeräten. Anlassbezogen finden zusätzliche Sensibilisierungsmaßnahmen statt, beispielsweise nach sicherheitsrelevanten Vorfällen oder bei neuen gesetzlichen Anforderungen. Die Teilnahme wird dokumentiert, um die Wirksamkeit der Maßnahme im Zeitverlauf nachvollziehen zu können.

   c. **Benannter Datenschutzbeauftragter:** Die CTO Balzuweit GmbH hat einen externen Datenschutzbeauftragten gemäß Art. 37 DSGVO bestellt. Diese Funktion wird durch die DataGAP GmbH wahrgenommen, die CTO in allen datenschutzrechtlichen Fragestellungen berät und die Einhaltung der DSGVO überwacht. Name und Kontaktdaten des Datenschutzbeauftragten sind öffentlich einsehbar und werden Kunden sowie Aufsichtsbehörden auf Anfrage mitgeteilt. Ein Wechsel des Datenschutzbeauftragten wird unverzüglich intern wie extern kommuniziert.

3. Datenschutz-Management (technisch)

   a. **Zentrale Datenschutzdokumentation:** Sämtliche Verfahrensweisen und Regelungen zum Datenschutz sind bei der CTO Balzuweit GmbH zentral dokumentiert und für Mitarbeitende über ein internes Wiki bzw. Intranet zugänglich. Der Zugriff erfolgt bedarfsorientiert entsprechend der jeweiligen Rolle und Aufgabe. Die Dokumentation umfasst unter anderem Richtlinien, Prozessbeschreibungen und Verantwortlichkeiten und wird regelmäßig aktualisiert. Damit ist sichergestellt, dass alle Mitarbeitenden jederzeit auf die für sie relevanten Datenschutzvorgaben zugreifen können.

   b. **Softwaregestütztes Datenschutz-Management:** Zur Steuerung und Dokumentation der Datenschutzorganisation setzt CTO die Datenschutz-Management-Software der DataGAP GmbH ein. Über dieses Tool werden unter anderem das Verzeichnis von Verarbeitungstätigkeiten, Risikobewertungen sowie Maßnahmen zur Umsetzung datenschutzrechtlicher Anforderungen gepflegt. Die Software unterstützt zudem die Nachverfolgung von Fristen, etwa im Zusammenhang mit Löschkonzepten oder Auftragsverarbeitungsverträgen. Durch den zentralen, softwaregestützten Ansatz wird eine konsistente und nachvollziehbare Umsetzung der Datenschutzanforderungen sichergestellt.

4. Datenschutzfreundliche Voreinstellungen (technisch)

   a. **Datenminimierung (Privacy by Default):** CTO berücksichtigt den Grundsatz der Datenminimierung sowohl bei der Entwicklung eigener Softwareprodukte als auch in internen Prozessen. Es werden grundsätzlich nur solche personenbezogenen Daten erhoben, gespeichert und verarbeitet, die für den jeweiligen Zweck tatsächlich erforderlich sind. Voreinstellungen in den CLARC-Produkten sind so gestaltet, dass standardmäßig ein datensparsamer Umgang mit personenbezogenen Daten gewährleistet ist. Bei der Konzeption neuer Funktionen wird die Erforderlichkeit der Datenerhebung regelmäßig überprüft und hinterfragt.

5. Eingabekontrolle (organisatorisch)

   a. **Berechtigungskonzept für Dateneingabe und -änderung:** Die Vergabe von Rechten zur Eingabe, Änderung und Löschung von Daten erfolgt bei CTO auf Basis eines dokumentierten Berechtigungskonzepts. Rechte werden ausschließlich entsprechend der jeweiligen Aufgabe und Funktion vergeben (Need-to-know-Prinzip). Das Berechtigungskonzept wird regelmäßig überprüft und bei organisatorischen Änderungen angepasst. Auf diese Weise wird sichergestellt, dass Änderungen an Daten stets nachvollziehbar einer berechtigten Person zugeordnet werden können.

   b. **Klare Löschzuständigkeiten:** Für die Löschung von Daten sind bei CTO klare Zuständigkeiten definiert, sodass jederzeit nachvollziehbar ist, wer für die Umsetzung von Löschanforderungen verantwortlich ist. Löschungen erfolgen auf Basis festgelegter Löschfristen bzw. auf begründete Anforderung, etwa im Rahmen von Betroffenenrechten. Die Durchführung wird dokumentiert, um die Einhaltung der Löschpflichten nachweisen zu können. Bei Unklarheiten hinsichtlich der Zuständigkeit greifen definierte Eskalationswege.

   c. **Individuelle Benutzerprofile:** Der Zugriff auf IT-Systeme erfolgt bei CTO ausschließlich über individuelle, personenbezogene Benutzerkonten und nicht über geteilte Gruppenkonten. Dadurch ist jede Eingabe, Änderung oder Löschung von Daten eindeutig einer natürlichen Person zuordenbar. Diese Nachvollziehbarkeit unterstützt sowohl interne Kontrollen als auch die Aufklärung im Falle von Sicherheitsvorfällen. Die Vergabe von Sammel- oder Funktionskonten ist nur in eng begrenzten, begründeten Ausnahmefällen vorgesehen.

   d. **Aufbewahrung von Ursprungsdokumente:** Dokumente, aus denen Daten in automatisierte Verarbeitungen übernommen wurden, werden bei CTO für einen angemessenen Zeitraum aufbewahrt. Dies ermöglicht im Bedarfsfall den Abgleich der elektronisch verarbeiteten Daten mit der ursprünglichen Eingabe. Die Aufbewahrung erfolgt unter Berücksichtigung geltender Aufbewahrungs- und Löschfristen. Nach Ablauf der jeweiligen Frist werden die Formulare datenschutzkonform vernichtet bzw. gelöscht.

   e. **Technische Protokollierung mittels Audit-Logs:** Ergänzend zum organisatorischen Berechtigungskonzept gewährleisten technische Audit-Logs die Nachvollziehbarkeit von Eingaben und Änderungen an Daten. Die Protokolle dokumentieren, wer wann welche Änderung vorgenommen hat, und stehen im Bedarfsfall für eine nachträgliche Auswertung zur Verfügung.

6. Incident-Response-Management (organisatorisch)

   a. **Meldeprozess für Sicherheitsvorfälle:** Für den Umgang mit Sicherheitsvorfällen und Datenschutzverletzungen verfolgt CTO in der Praxis bereits ein gewachsenes, strukturiertes Vorgehen zur Erkennung, Bewertung und Meldung solcher Vorfälle. Ein eigenständiger, formal dokumentierter Prozess besteht hierfür bislang nicht; im Zuge der laufenden

ISO/IEC-27001-Zertifizierung wird dieses Vorgehen nun dokumentiert und förmlich eingeführt – einschließlich klar definierter Zuständigkeiten für die Bewertung und der Fristen für eine etwaige Meldung an die zuständige Aufsichtsbehörde gemäß Art. 33 DSGVO. Mitarbeitende werden bereits heute für die Erkennung möglicher Anzeichen eines Sicherheitsvorfalls sensibilisiert. Nach der Einführung wird der Prozess einer regelmäßigen Überprüfung und kontinuierlichen Weiterentwicklung anhand von Erfahrungswerten unterzogen.

b. **Einbindung von Datenschutz- und Informationssicherheitsbeauftragtem:** Im Falle eines Sicherheitsvorfalls oder einer Datenschutzverletzung werden sowohl der Datenschutzbeauftragte als auch der Informationssicherheitsbeauftragte von CTO unverzüglich eingebunden. Sie unterstützen bei der Bewertung des Risikos für die betroffenen Personen sowie bei der Entscheidung über erforderliche Meldepflichten. Beide Funktionen wirken zudem an der Nachbereitung des Vorfalls und der Ableitung von Verbesserungsmaßnahmen mit. Dadurch wird sichergestellt, dass rechtliche und technische Aspekte eines Vorfalls gemeinsam bewertet werden.

7. Incident-Response-Management (technisch)

a. **Firewall-Systeme:** Zum Schutz vor unbefugtem Netzwerkzugriff setzt CTO Firewall-Systeme ein, die den Datenverkehr zwischen internen Systemen und dem Internet kontrollieren und filtern. Es werden ausschließlich die für den Betrieb zwingend erforderlichen Ports und Dienste freigegeben. Die Firewall-Konfiguration wird regelmäßig überprüft und an aktuelle Schutzbedarfe angepasst. Sicherheitsrelevante Updates der Firewall-Systeme werden zeitnah eingespielt. Die eingesetzten Systeme kombinieren klassische Firewall-Funktionalität mit Intrusion-Detection- und -Prevention-Mechanismen; bei CLARC-Cloud-Lösungen sind grundsätzlich nur die für den jeweiligen Dienst zwingend erforderlichen Ports freigeschaltet, beispielsweise Port 443 für HTTPS.

b. **Spam- und Phishing-Schutz:** Eingehende E-Mails werden bei CTO automatisiert über eine Spam- und Phishing-Schutzlösung geprüft, um Schadsoftware sowie betrügerische Nachrichten frühzeitig herauszufiltern. Die zugrunde liegenden Filterregeln und Signaturen werden regelmäßig aktualisiert. Verdächtige E-Mails werden entsprechend markiert bzw. blockiert, bevor sie den Empfänger erreichen. Mitarbeitende werden ergänzend für die Erkennung von Phishing-Versuchen sensibilisiert.

c. **Virenschutz:** Alle produktiv genutzten Endgeräte und Server der CTO Balzuweit GmbH sind mit einer Antiviren-Lösung ausgestattet, die kontinuierlich im Hintergrund arbeitet. Die Signaturen und Erkennungsmechanismen werden automatisiert und regelmäßig aktualisiert, um auch neue Bedrohungen zu erkennen. Erkannte Schadsoftware wird automatisch isoliert bzw. entfernt und die zuständigen Administratoren informiert. Der Status des Virenschutzes wird zentral überwacht. Zum Einsatz kommt dabei eine moderne Endpoint-Detection-Lösung, die über die signaturbasierte Erkennung hinaus auch verdächtiges Verhalten auf den Endgeräten erkennt.

d. **Intrusion-Prevention-System (IPS):** Ergänzend zu klassischen Firewall-Maßnahmen setzt CTO ein Intrusion-Prevention-System ein, das den Netzwerkverkehr auf verdächtige Muster und Angriffsversuche überwacht. Erkannte Angriffsversuche werden automatisiert blockiert, bevor sie Schaden verursachen können. Auffälligkeiten werden protokolliert und im Bedarfsfall durch die zuständigen Mitarbeitenden ausgewertet. Das System wird kontinuierlich an aktuelle Bedrohungsszenarien angepasst.

e. **Patch- und Update-Management:** Produktive IT-Systeme werden bei CTO regelmäßig mit Updates versorgt. Sicherheitsupdates für Endgeräte werden zeitnah nach ihrem Erscheinen eingespielt, zentrale IT-Systeme und CLARC-Cloud-Lösungen werden in geplanten

Wartungsfenstern aktualisiert. Werden außerplanmäßig kritische Sicherheitslücken bekannt, erfolgt das Einspielen der entsprechenden Patches umgehend außerhalb des regulären Wartungsfensters.

f. **Schwachstellen- und Belastbarkeitstests:** CTO führt regelmäßig Schwachstellenscans sowie Belastbarkeitstests durch, um Sicherheitslücken und Kapazitätsengpässe frühzeitig zu erkennen. Festgestellte Schwachstellen werden bewertet und entsprechend ihrer Kritikalität priorisiert behoben. Die Ergebnisse fließen in die kontinuierliche Verbesserung der technischen Schutzmaßnahmen ein.

8. Transport- und Weitergabekontrolle (organisatorisch)

   a. **Sorgfältige Auswahl bei physischem Transport:** Sofern in Ausnahmefällen ein physischer Transport von Datenträgern oder Unterlagen erforderlich ist, erfolgt die Auswahl des Transportpersonals sowie der eingesetzten Fahrzeuge bei CTO unter besonderer Sorgfalt. Es werden nur vertrauenswürdige, vertraglich gebundene Dienstleister beauftragt. Transportbehälter werden so gewählt, dass ein unbefugter Zugriff während des Transports ausgeschlossen ist. Der überwiegende Teil des Datenaustauschs erfolgt jedoch elektronisch über verschlüsselte Kommunikationswege, sodass physische Transporte die Ausnahme darstellen.

9. Transport- und Weitergabekontrolle (technisch)

   a. **VPN-Verschlüsselung:** Für die Übertragung von Daten über öffentliche oder unternehmensübergreifende Netzwerke setzt CTO VPN-Technologie ein. Dadurch wird eine verschlüsselte Verbindung zwischen den beteiligten Systemen hergestellt, die ein Mitlesen oder Manipulieren der übertragenen Daten durch Dritte verhindert. VPN-Verbindungen kommen insbesondere bei Remote-Zugriffen von Mitarbeitenden sowie bei der Anbindung von Kundensystemen zum Einsatz. Die eingesetzten Verschlüsselungsverfahren orientieren sich am aktuellen Stand der Technik.

   b. **E-Mail-Verschlüsselung:** Für den E-Mail-Verkehr nutzt CTO Verschlüsselungstechnologien, um die Vertraulichkeit der übermittelten Inhalte zu schützen. Die Transportverschlüsselung erfolgt standardmäßig; bei besonders sensiblen Inhalten kann darüber hinaus eine zusätzliche Inhaltsverschlüsselung vereinbart werden. Mitarbeitende werden im Umgang mit vertraulichen Informationen im E-Mail-Verkehr geschult. Der Versand hochsensibler Daten per unverschlüsselter E-Mail wird vermieden.

   c. **Verschlüsselte Datenübertragungswege:** Die Bereitstellung von Daten und Dokumenten erfolgt bei CTO ausschließlich über verschlüsselte Verbindungen, beispielsweise mittels SFTP oder HTTPS. Unverschlüsselte Übertragungswege wie einfaches FTP oder HTTP kommen für die Übertragung personenbezogener oder vertraulicher Daten nicht zum Einsatz. Die eingesetzten Verschlüsselungsprotokolle und Zertifikate werden regelmäßig auf ihre Aktualität geprüft. Damit ist sichergestellt, dass Daten auf dem Übertragungsweg wirksam vor unbefugter Kenntnisnahme geschützt sind.

   d. **Verschlüsselung von Website und Web-Anwendungen:** Alle von außen erreichbaren Webseiten und Web-Anwendungen der CTO Balzuweit GmbH, einschließlich der CLARC-Cloud-Angebote, sind ausschließlich über eine verschlüsselte HTTPS-Verbindung erreichbar. Die eingesetzten TLS-Zertifikate werden regelmäßig erneuert und die Verschlüsselungskonfiguration am Stand der Technik ausgerichtet. Unverschlüsselte Zugriffe werden automatisch auf die verschlüsselte Verbindung umgeleitet bzw. abgelehnt. Dadurch werden die Vertraulichkeit und Integrität der übertragenen Daten sichergestellt. Die eingesetzten Verschlüsselungsverfahren orientieren sich an den Vorgaben der technischen Richtlinie BSI TR-02102 des Bundesamts für Sicherheit in der Informationstechnik.

e. **Sichere Transportbehälter:** Müssen in Ausnahmefällen Datenträger oder vertrauliche Unterlagen physisch transportiert werden, kommen bei CTO gesicherte, verschließbare Transportbehälter zum Einsatz. Diese verhindern den unbefugten Zugriff während des Transports und machen eine unbemerkte Manipulation erkennbar. Der Einsatz solcher Behälter erfolgt insbesondere beim Transport von Datenträgern mit besonders sensiblen Inhalten. Die überwiegende Datenübertragung erfolgt jedoch, wie beschrieben, elektronisch und verschlüsselt.

f. **Verschlüsselung von Datenträgern:** Datenträger von Notebooks sowie extern genutzte Datenträger werden bei CTO, soweit technisch möglich, verschlüsselt. Dabei kommen die im jeweiligen Betriebssystem integrierten Verschlüsselungsverfahren zum Einsatz, etwa Microsoft BitLocker. Dadurch bleiben Daten auf verloren gegangenen oder gestohlenen Geräten vor unbefugtem Zugriff geschützt.

10. Trennungskontrolle (organisatorisch)

a. **Festlegung von Datenbankrechten:** Der Zugriff auf Datenbanken wird bei CTO über ein rollenbasiertes Rechtekonzept gesteuert, das festlegt, welche Personen bzw. Systeme auf welche Daten zugreifen dürfen. Die Vergabe der Rechte orientiert sich am Erforderlichkeitsprinzip und wird dokumentiert. Änderungen an Datenbankrechten werden nachvollziehbar protokolliert. Die Rechtevergabe wird regelmäßig überprüft und bei Bedarf angepasst, etwa bei Änderungen von Aufgabenbereichen.

11. Trennungskontrolle (technisch)

a. **Getrennte Aufbewahrung nach Verarbeitungszweck:** Physische und elektronische Daten aus einer Verarbeitungstätigkeit werden bei CTO organisatorisch und technisch von Datensätzen anderer Zwecke bzw. anderer Kunden getrennt aufbewahrt. Dadurch wird eine Vermischung von Daten unterschiedlicher Verarbeitungszwecke verhindert. Die Trennung wird sowohl auf Datenbankebene als auch bei der Ablage von Dokumenten umgesetzt. Zugriffsrechte werden entsprechend der jeweiligen Trennung vergeben.

b. **Physikalische Systemtrennung:** Kritische Systeme, Datenbanken und Datenträger werden bei CTO, soweit erforderlich, physikalisch voneinander getrennt betrieben. Dies reduziert das Risiko, dass sich ein Sicherheitsvorfall unkontrolliert von einem System auf weitere Systeme ausbreitet. Die physikalische Trennung ergänzt die logische Trennung auf Anwendungs- und Datenbankebene. Die Ausgestaltung richtet sich nach dem jeweiligen Schutzbedarf der verarbeiteten Daten.

c. **Mandantenfähigkeit der Anwendungen:** Die von CTO betriebenen Cloud-Lösungen, insbesondere CLARC Infinity, sind mandantenfähig ausgelegt. Jeder Mandant erhält eine eindeutige Kennung, die bei jedem Systemzugriff verifiziert wird, um eine strikte Trennung der Daten zwischen unterschiedlichen Kunden sicherzustellen. Ein Zugriff auf Daten anderer Mandanten ist durch diese technische Trennung ausgeschlossen. Die Mandantentrennung wird regelmäßig im Rahmen von Tests und Reviews überprüft. Ein Mandant entspricht dabei in der Regel einem Kunden mit mehreren zugehörigen Nutzerkonten.

12. Verfügbarkeitskontrolle (organisatorisch)

a. **Protokollierung des Sicherungsvorgangs:** Die Durchführung von Datensicherungen wird bei CTO protokolliert und regelmäßig kontrolliert. Fehlgeschlagene Sicherungsläufe werden automatisiert gemeldet und zeitnah nachverfolgt. Die Protokolle ermöglichen eine nachträgliche Überprüfung, ob Sicherungen vollständig und im vorgesehenen Zeitfenster durchgeführt wurden. Stichprobenartig werden Wiederherstellungen aus Backups getestet, um die tatsächliche Funktionsfähigkeit der Sicherungen sicherzustellen. Häufigkeit

und Aufbewahrungsdauer der Sicherungen richten sich nach der Sensibilität der jeweils gesicherten Daten; für CLARC-Cloud-Lösungen sind die konkreten Sicherungsintervalle und Aufbewahrungszeiten den jeweiligen Leistungsbeschreibungen zu entnehmen.

b. **Getrennte Partitionen für Betriebssystem und Daten:** Je nach Anforderung und Schutzniveau werden Server bei CTO möglichst so konfiguriert, dass Betriebssystem und Nutzdaten auf getrennten Partitionen bzw. Datenträgern liegen. Dies erleichtert im Störungsfall die gezielte Wiederherstellung einzelner Bereiche, ohne dass produktive Daten unnötig gefährdet werden. Die Trennung unterstützt zudem eine effizientere Datensicherung und Systemwartung. Die Konfiguration ist Bestandteil der internen Systemstandards für den Serverbetrieb.

c. **Dezentrale Aufbewahrung von Sicherungsmedien:** Sicherungsmedien werden bei CTO nicht ausschließlich am Standort der produktiven Systeme aufbewahrt, sondern zusätzlich an einem separaten, gesicherten Ort vorgehalten. Dadurch bleibt im Falle eines lokalen Schadensereignisses, etwa eines Brand- oder Wasserschadens im Serverraum, eine unabhängige Kopie der Daten verfügbar. Der Zugriff auf die extern aufbewahrten Sicherungsmedien ist auf einen begrenzten Personenkreis beschränkt. Die räumliche Trennung ist fester Bestandteil des Notfallkonzepts.

d. **Schutz der Serverräume vor Wasserschäden:** Innerhalb und oberhalb der von CTO genutzten Serverräume befinden sich keine sanitären Anschlüsse, um das Risiko von Wasserschäden an IT-Systemen zu minimieren. Die bauliche Gestaltung der Serverräume berücksichtigt zusätzliche Schutzmaßnahmen gegen Feuchtigkeit. Bestehende Risiken werden im Rahmen der Gebäude- und Infrastrukturplanung regelmäßig überprüft. Für Cloud-Lösungen, die bei zertifizierten Rechenzentrumsbetreibern gehostet werden, gelten zusätzlich die baulichen Schutzmaßnahmen des jeweiligen Rechenzentrumsbetreibers.

13. Verfügbarkeitskontrolle (technisch)

a. **Festplattenspiegelung (RAID):** Server der CTO Balzuweit GmbH sind mit RAID-Systemen ausgestattet, die eine Spiegelung der gespeicherten Daten auf mehreren physischen Festplatten vorsehen. Fällt eine einzelne Festplatte aus, bleibt der Zugriff auf die Daten durch die redundante Speicherung weiterhin gewährleistet. Der Zustand der RAID-Systeme wird über ein Monitoring überwacht, sodass defekte Komponenten zeitnah erkannt und ausgetauscht werden können. Dies trägt wesentlich zur Verfügbarkeit und Belastbarkeit der IT-Systeme bei.

b. **Brandfrüherkennung im Serverraum:** Die von CTO betriebenen Serverräume sind mit Feuer- und Rauchmeldeanlagen ausgestattet, die eine frühzeitige Erkennung eines Brandereignisses ermöglichen. Im Alarmfall werden automatisch die zuständigen Stellen informiert, sodass unverzüglich reagiert werden kann. Die Anlagen werden regelmäßig gewartet und auf Funktionsfähigkeit geprüft. Die Maßnahme dient dem Schutz von Hardware, Daten und letztlich der Verfügbarkeit der IT-Systeme.

c. **Klimatisierung des Serverraums:** Die Serverräume der CTO Balzuweit GmbH sind klimatisiert, um eine für den Betrieb der IT-Systeme geeignete Temperatur konstant zu gewährleisten. Eine gleichbleibende Betriebstemperatur reduziert das Risiko von Hardwareausfällen durch Überhitzung. Die Klimatisierung wird durch eine Temperaturüberwachung ergänzt, sodass Abweichungen zeitnah erkannt werden. Wartung und Prüfung der Klimatechnik erfolgen in regelmäßigen Intervallen.

d. **Überspannungsschutz im Serverraum:** Im Serverraum eingesetzte Schutzsteckdosenleisten sichern die angeschlossenen IT-Systeme gegen Überspannungen und Spannungsspitzen ab. Dies reduziert das Risiko von Hardwareschäden durch elektrische Störungen im Stromnetz. Die Schutzsteckdosenleisten sind Teil des umfassenderen Konzepts zur

Absicherung der Stromversorgung im Serverraum, das auch die unterbrechungsfreie Stromversorgung umfasst. Die Funktionsfähigkeit wird im Rahmen regelmäßiger Prüfungen der technischen Infrastruktur kontrolliert.

e. **Überwachung von Temperatur und Feuchtigkeit:** Der Serverraum wird kontinuierlich mittels Sensoren auf Temperatur und Luftfeuchtigkeit überwacht. Bei Abweichungen von den definierten Sollwerten werden automatisiert Warnmeldungen an die zuständigen Mitarbeitenden ausgelöst. Dies ermöglicht ein frühzeitiges Eingreifen, bevor es zu Beeinträchtigungen der IT-Systeme kommt. Die Überwachungsdaten werden protokolliert und stehen für eine nachträgliche Auswertung zur Verfügung.

f. **Unterbrechungsfreie Stromversorgung (USV):** Zur Absicherung gegen kurzzeitige Stromausfälle setzt CTO eine unterbrechungsfreie Stromversorgung für die Computersysteme im Serverraum ein. Die USV überbrückt kurze Unterbrechungen der Stromversorgung und ermöglicht bei längeren Ausfällen ein kontrolliertes Herunterfahren der Systeme. Die Kapazität und Funktionsfähigkeit der USV-Anlage werden regelmäßig getestet. Dadurch wird das Risiko von Datenverlusten durch abrupte Stromausfälle deutlich reduziert.

g. **Alarmierung bei unbefugtem Zutritt zum Serverraum:** Der Serverraum ist zusätzlich zur regulären Zutrittskontrolle mit einer Zutrittsmeldeanlage ausgestattet, die einen unberechtigten Zutrittsversuch automatisch meldet. Ein entsprechender Alarm wird unmittelbar an die zuständigen Mitarbeitenden bzw. eine Sicherheitszentrale weitergeleitet. Dies ermöglicht ein zeitnahes Eingreifen im Falle eines unbefugten Zutrittsversuchs. Die Anlage wird regelmäßig auf Funktionsfähigkeit geprüft.

h. **Monitoring und Alarmierung der IT-Systeme:** Für die Überwachung der IT-Systeme setzt CTO ein Monitoring- und Alarmierungssystem ein. Definierte Alarme informieren die zuständigen Mitarbeitenden automatisiert über Abweichungen vom Normalbetrieb. Dadurch werden Störungen frühzeitig erkannt und die Zeit bis zur Wiederherstellung des Normalbetriebs verkürzt.

i. **Redundante Auslegung kritischer Systeme:** Kritische IT-Systeme sind bei CTO, soweit wirtschaftlich und technisch sinnvoll, redundant ausgelegt. Fällt eine Komponente aus, kann der Betrieb dadurch ohne Unterbrechung fortgesetzt werden. Die Redundanzkonzepte werden regelmäßig überprüft und an den jeweiligen Schutzbedarf angepasst.

14. Zugangskontrolle (organisatorisch)

a. **Zentrale Verwaltung von Benutzerberechtigungen:** Benutzerberechtigungen für IT-Systeme werden bei CTO zentral verwaltet. Die Vergabe erfolgt im Rahmen eines definierten Freigabeprozesses, der bei Eintritt neuer Mitarbeitender startet und bei Austritt oder Rollenwechsel entsprechend angepasst bzw. entzogen wird. Die zentrale Verwaltung erleichtert regelmäßige Überprüfungen der vergebenen Berechtigungen. Abweichungen von der Soll-Konfiguration können dadurch zeitnah erkannt und korrigiert werden. Die Anlage der Benutzerkonten sowie die initiale Vergabe von Zugangsberechtigungen erfolgt im Rahmen des Onboarding-Prozesses, der durch das HR-Team angestoßen wird; die Freigabe obliegt der Geschäftsleitung. Die Vergabe weiterer Zugangsberechtigungen erfolgt, wo möglich, grundsätzlich schriftlich.

b. **Verwaltung von Benutzerrechten:** Über die zentrale Vergabe hinaus werden Benutzerrechte bei CTO fortlaufend verwaltet und an aktuelle Aufgaben angepasst. Nicht mehr benötigte Rechte werden zeitnah entzogen, um das Prinzip der minimalen Rechtevergabe einzuhalten. Änderungen an Benutzerrechten werden dokumentiert und sind nachvollziehbar. Die Verwaltung erfolgt in enger Abstimmung zwischen IT und den jeweiligen Fachbereichen.

c. **Richtlinie zum Umgang mit mobilen Geräten:** Für die Nutzung mobiler Endgeräte, wie Notebooks oder Smartphones, besteht bei CTO eine verbindliche interne Richtlinie. Sie regelt unter anderem Anforderungen an die Absicherung der Geräte, den Umgang mit dienstlichen Daten unterwegs sowie das Verhalten bei Verlust oder Diebstahl. Mitarbeitende werden im Rahmen des Onboardings sowie bei Bedarf erneut über die Inhalte der Richtlinie belehrt. Die Einhaltung der Richtlinie ist Voraussetzung für die Nutzung mobiler Geräte im dienstlichen Kontext.

d. **Richtlinie für Home-Office und mobiles Arbeiten:** Home-Office und mobiles Arbeiten sind bei CTO nur im Rahmen einer verbindlichen internen Richtlinie zulässig. Diese stellt sicher, dass der jeweilige Arbeitsplatz die erforderlichen Vertraulichkeitsanforderungen erfüllt, etwa hinsichtlich der sicheren Aufbewahrung von Unterlagen und Endgeräten sowie der Nutzung privater Hardware. Mitarbeitende verpflichten sich zur Einhaltung dieser Vorgaben. Besondere, darüberhinausgehende Anforderungen einzelner Auftraggeber werden bei Bedarf zusätzlich berücksichtigt. Die Richtlinie sieht insbesondere vor, dass die Nutzung privater Hardware auf ein Minimum wie Internetanschluss, Peripheriegeräte oder Monitore begrenzt wird, dass Unterlagen und Datenträger nicht unterwegs oder im Home-Office entsorgt, sondern in die Geschäftsräume zurückgebracht werden, und dass dienstliche Endgeräte stets sicher zu verwahren sind.

e. **Regelmäßige Leerung der Postfächer:** Physische Posteingänge werden bei CTO regelmäßig geleert, um eine unnötige Ansammlung vertraulicher Unterlagen zu vermeiden. Dies reduziert das Risiko, dass unbefugte Personen Einblick in eingegangene Post erhalten. Die Zuständigkeit für die Leerung ist organisatorisch klar geregelt. Eingehende Post mit personenbezogenen Daten wird zeitnah an die zuständigen Stellen weitergeleitet.

f. **Verschlossene Postfächer:** Die physischen Postfächer der CTO Balzuweit GmbH sind verschließbar ausgeführt, sodass ein unbefugter Zugriff auf eingegangene Post ausgeschlossen ist. Der Zugang zu den Postfächern ist auf berechtigte Personen beschränkt. Dies gilt insbesondere für Post mit vertraulichem oder personenbezogenem Inhalt. Die Maßnahme ergänzt die organisatorischen Vorgaben zur regelmäßigen Leerung der Postfächer.

g. **Vertrauliche Telefonate:** Telefonate mit vertraulichem oder personenbezogenem Inhalt werden bei CTO grundsätzlich hinter verschlossener Tür geführt. Dadurch wird verhindert, dass unbeteiligte Personen Gesprächsinhalte mithören können. Mitarbeitende sind entsprechend sensibilisiert, insbesondere in Großraum- oder Gemeinschaftsbüros auf diese Anforderung zu achten. Die Vorgabe gilt gleichermaßen im Büro wie im Home-Office.

h. **Vertrauliche Videokonferenzen:** Videokonferenzen mit vertraulichen Inhalten werden bei CTO grundsätzlich hinter verschlossener Tür und mit Sichtschutz durchgeführt. So wird verhindert, dass Bildschirminhalte oder Gesprächsinhalte von unbeteiligten Dritten eingesehen oder mitgehört werden können. Bei der Nutzung von Videokonferenzsystemen wird zudem auf eine sichere Konfiguration geachtet, etwa durch Zugangsbeschränkungen für einzelne Meetings. Mitarbeitende werden entsprechend für den vertraulichen Umgang mit Videokonferenzen sensibilisiert.

15. Zugangskontrolle (technisch)

a. **Virenschutz auf Clients:** Alle Client-Arbeitsplätze der CTO Balzuweit GmbH sind mit einer Antiviren-Lösung ausgestattet. Die Aktualisierung der Virensignaturen erfolgt automatisiert im Hintergrund, um einen durchgehenden Schutz sicherzustellen. Erkannte Bedrohungen werden automatisch isoliert bzw. entfernt und protokolliert. Der Status des Virenschutzes wird zentral überwacht, sodass Abweichungen zeitnah auffallen.

b. **Virenschutz auf Servern:** Auch die Serverlandschaft der CTO Balzuweit GmbH ist durch eine entsprechende Antiviren-Lösung geschützt. Die Signaturen und Erkennungsmechanismen werden regelmäßig automatisiert aktualisiert. Server-Scans werden in für den Betrieb unkritischen Zeitfenstern durchgeführt, um Beeinträchtigungen des laufenden Betriebs zu vermeiden. Auffälligkeiten werden zentral protokolliert und ausgewertet.

c. **Automatische Bildschirmsperre:** Arbeitsplatzrechner sperren sich bei CTO nach einer definierten Zeit der Inaktivität automatisch, sodass ein unbeaufsichtigter Zugriff auf angemeldete Sitzungen verhindert wird. Zur erneuten Anmeldung ist die Eingabe des persönlichen Passworts bzw. eines anderen Faktors erforderlich. Mitarbeitende sind zusätzlich angewiesen, ihren Arbeitsplatz beim Verlassen unabhängig von der automatischen Sperre selbst zu sperren. Die Einstellung der automatischen Sperre ist zentral vorgegeben und kann von Mitarbeitenden nicht eigenständig deaktiviert werden. Die automatische Sperre greift dabei spätestens nach zehn Minuten Inaktivität.

d. **Personalisierte Anmeldung:** Die Anmeldung an IT-Systemen erfolgt bei CTO über personalisierte Benutzerkonten mit Benutzername und Passwort. Geteilte oder anonyme Zugänge werden für den produktiven Betrieb nicht eingesetzt. Die Anmeldedaten werden von den Mitarbeitenden vertraulich behandelt und nicht an Dritte weitergegeben. Wo technisch möglich, wird die Anmeldung durch zusätzliche Sicherheitsmechanismen wie eine Multi-Faktor-Authentifizierung ergänzt. Als zentraler Verzeichnisdienst für die Anmeldung an den produktiven Systemen und Servern setzt CTO Microsoft Active Directory ein.

e. **Zuordnung von Berechtigungen zu IT-Systemen:** Benutzerprofile werden bei CTO gezielt den IT-Systemen zugeordnet, die für die jeweilige Tätigkeit erforderlich sind. Eine pauschale Vergabe von Zugriffsrechten auf alle Systeme findet nicht statt. Die Zuordnung wird bei Änderungen der Tätigkeit oder des Aufgabenbereichs entsprechend angepasst. Regelmäßige Überprüfungen stellen sicher, dass die vergebenen Berechtigungen weiterhin dem tatsächlichen Bedarf entsprechen.

f. **Intrusion-Detection-System (IDS):** Zur Erkennung von Angriffsversuchen auf das Netzwerk setzt CTO ein Intrusion-Detection-System ein, das den Datenverkehr kontinuierlich auf auffällige Muster überwacht. Bei Erkennung verdächtiger Aktivitäten werden automatisiert Warnmeldungen ausgelöst. Die zuständigen Mitarbeitenden bewerten die Meldungen und leiten bei Bedarf weitere Maßnahmen ein. Das System ergänzt die präventiven Maßnahmen von Firewall und Intrusion-Prevention-System um eine kontinuierliche Überwachungskomponente.

g. **Mobile Device Management:** Dienstlich genutzte Smartphones und Tablets werden bei CTO über eine zentrale Mobile-Device-Management-Lösung verwaltet. Über diese Lösung können unter anderem Sicherheitsrichtlinien durchgesetzt sowie im Falle von Verlust oder Diebstahl Daten auf dem Gerät aus der Ferne gelöscht werden. Die Einbindung eines Geräts in das Mobile Device Management ist Voraussetzung für den Zugriff auf dienstliche Daten. Die Konfiguration der Geräte wird zentral überwacht und bei Bedarf angepasst.

h. **Passwortgeschützter Zugang:** Der Zugang zu IT-Systemen der CTO Balzuweit GmbH ist durchgängig durch ein Passwort geschützt. Es gelten interne Vorgaben zur Passwortkomplexität, die sich am aktuellen Stand der Technik und den Empfehlungen anerkannter Stellen orientieren. Passwörter werden ausschließlich verschlüsselt gespeichert und nicht im Klartext übertragen. Mitarbeitende werden zum sorgfältigen Umgang mit ihren Zugangsdaten angehalten.

i. **Umfassender Virenschutz:** Ergänzend zu den systemspezifischen Regelungen für Clients und Server verfolgt CTO einen unternehmensweiten Ansatz beim Virenschutz, der alle produktiv genutzten Endgeräte einbezieht. Die eingesetzten Lösungen werden zentral gesteuert und überwacht. Updates und Signaturaktualisierungen erfolgen automatisiert.

Der Virenschutz ist damit integraler Bestandteil des Schutzkonzepts gegen Schadsoftware.

j. **VPN für den Fernzugriff:** Der Zugriff von Mitarbeitenden auf interne Systeme von unterwegs oder aus dem Home-Office erfolgt bei CTO ausschließlich über eine verschlüsselte VPN-Verbindung. Dadurch wird sichergestellt, dass auch außerhalb der Geschäftsräume ein dem internen Netzwerk vergleichbares Schutzniveau besteht. Der Zugang zum VPN ist an eine erfolgreiche Authentifizierung des jeweiligen Mitarbeitenden gebunden. Die eingesetzte VPN-Technologie wird regelmäßig auf dem aktuellen Stand der Technik gehalten.

k. **Verschlüsselung mobiler Endgeräte:** Dienstlich genutzte Smartphones werden bei CTO, soweit technisch möglich, verschlüsselt betrieben. Dadurch bleiben auf dem Gerät gespeicherte Daten im Falle eines Verlusts oder Diebstahls vor unbefugtem Zugriff geschützt. Die Verschlüsselung wird in Kombination mit einer Geräte- bzw. Bildschirmsperre eingesetzt. Die Einhaltung dieser Vorgabe wird über die Mobile-Device-Management-Lösung sichergestellt.

l. **Single-Sign-On (SSO):** Unterstützt ein von CTO eingesetztes IT-System Single-Sign-On, wird dieser Mechanismus verpflichtend aktiviert. Dadurch melden sich Mitarbeitende einmalig zentral an und erhalten darüber Zugriff auf berechtigte Anwendungen, ohne Zugangsdaten mehrfach verwalten zu müssen. Dies reduziert das Risiko unsicherer, mehrfach verwendeter Passwörter. Der zentrale Anmeldeprozess erleichtert zudem die Deaktivierung von Zugängen bei Austritt eines Mitarbeitenden.

m. **Multi-Faktor-Authentifizierung (MFA):** Die Aufforderung zur Eingabe eines zweiten Faktors erfolgt bei CTO abhängig davon, von welchem Endgerät der Zugriff erfolgt und welchen Schutzbedarf das jeweilige IT-System aufweist. Insbesondere bei Zugriffen von außerhalb des internen Netzwerks oder auf besonders schützenswerte Systeme wird eine Multi-Faktor-Authentifizierung eingesetzt. Dadurch bleibt ein Konto auch bei Kompromittierung des Passworts allein durch einen Dritten nicht unmittelbar zugänglich. CTO setzt die Multi-Faktor-Authentifizierung, wo technisch möglich, konsequent für administrative Zugänge sowie Cloud-Dienste ein.

n. **Zugang zu Cloud-Lösungen:** Der Zugang zu den CLARC-Cloud-Lösungen erfolgt ausschließlich über personalisierte Benutzerkonten unter Anwendung der zuvor beschriebenen Sicherheitsmaßnahmen. Wo technisch möglich, werden für automatisierte Prozesse eingeschränkte, auf das notwendige Minimum reduzierte Serviceaccounts anstelle persönlicher Zugänge verwendet. Dies reduziert das Risiko im Falle einer Kompromittierung einzelner Zugangsdaten.

o. **Protokollierung von Zugangsversuchen zu Cloud-Produkten:** Erfolgreiche und fehlgeschlagene administrative Zugangsversuche zu den CLARC-Cloud-Lösungen werden dauerhaft protokolliert. Die Protokolle stehen für eine Auswertung zur Verfügung und werden stichprobenartig sowie anlassbezogen, etwa bei Verdacht auf unbefugte Zugriffe, ausgewertet. Auffällige Zugriffsmuster lassen sich auf diese Weise auch nachträglich nachvollziehen.

p. **Verschlüsselung und Segmentierung von WLAN-Netzwerken:** Funknetzwerke, über die interne Systeme erreichbar sind, kommunizieren bei CTO ausschließlich verschlüsselt. Die WLAN-Infrastruktur ist in getrennte Netzwerke für Mitarbeitende und für Gäste aufgeteilt. Aus einem Gäste-WLAN besteht kein Zugriff auf interne IT-Systeme.

16. Zugriffskontrolle/Pseudonymisierung (organisatorisch)

a. **Minimale Anzahl an Administratoren:** Die Anzahl der Mitarbeitenden mit besonderen administrativen Zugriffsberechtigungen wird bei CTO bewusst geringgehalten. Administrative Rechte werden nur an Personen vergeben, die diese für ihre konkrete Tätigkeit zwin-

gend benötigen. Die Vergabe und Nutzung administrativer Berechtigungen werden zusätzlich protokolliert. Regelmäßige Überprüfungen stellen sicher, dass keine nicht mehr benötigten administrativen Rechte bestehen bleiben.

b. **Zugriff nur für autorisiertes Personal:** Der Zugriff auf Systeme und Daten ist bei CTO ausschließlich dafür autorisiertem Personal vorbehalten. Die Autorisierung erfolgt im Rahmen des zentralen Berechtigungskonzepts und wird dokumentiert. Nicht autorisierte Zugriffsversuche werden technisch unterbunden bzw. protokolliert. Die Autorisierung wird regelmäßig überprüft und bei Bedarf angepasst.

c. **Trennung von Produktiv- und Testumgebung:** CTO trennt Produktiv- und Testumgebungen konsequent voneinander. Neue Softwareversionen und Änderungen werden zunächst in der Testumgebung geprüft, bevor sie in die Produktivumgebung übernommen werden. Der Zugriff auf beide Umgebungen ist mit jeweils eigenen, bedarfsgerechten Berechtigungen versehen. Diese Trennung verhindert, dass Testaktivitäten unbeabsichtigt Auswirkungen auf produktive Daten oder Systeme haben. Für CLARC-Cloud-Lösungen ist zusätzlich ein mehrstufiger Deployment-Prozess etabliert: Änderungen werden dokumentiert und versioniert, zunächst in der Testumgebung geprüft und erst nach einer internen Qualitätsfreigabe in die Produktivumgebung übernommen.

d. **Definiertes Berechtigungskonzept:** Der Zugriff auf IT-Systeme und Anwendungen basiert bei CTO auf einem definierten, dokumentierten Berechtigungskonzept. Es legt fest, welche Rollen welche Zugriffsrechte auf welche Daten und Funktionen erhalten. Das Konzept wird regelmäßig überprüft und an organisatorische oder technische Änderungen angepasst. Abweichungen von der Soll-Berechtigung werden im Rahmen von Rezertifizierungen identifiziert und korrigiert. Die Vergabe zusätzlicher, über die Grundausstattung hinausgehender Zugriffsberechtigungen erfolgt grundsätzlich schriftlich.

17. Zugriffskontrolle/Pseudonymisierung (technisch)

a. **Vernichtung geheimhaltungsbedürftiger Unterlagen (Sicherheitsstufe 5):** Für die Vernichtung von Unterlagen mit besonders geheimhaltungsbedürftigen personenbezogenen Daten setzt CTO Aktenvernichter der Sicherheitsstufe 5 im Cross-Cut-Verfahren ein. Diese hohe Sicherheitsstufe gewährleistet eine besonders feine Zerkleinerung, sodass eine Rekonstruktion der Inhalte praktisch ausgeschlossen ist. Der Einsatz dieser Stufe erfolgt gezielt bei entsprechend eingestuften Unterlagen. Die Vernichtung wird dokumentiert.

b. **Vernichtung sonstiger vertraulicher Unterlagen (Sicherheitsstufe 3):** Für die laufende Vernichtung vertraulicher, aber nicht besonders geheimhaltungsbedürftiger Unterlagen setzt CTO Aktenvernichter mit mindestens Sicherheitsstufe 3 im Cross-Cut-Verfahren ein. Diese Geräte stehen an geeigneten Standorten im Unternehmen zur Verfügung. Mitarbeitende sind angehalten, vertrauliche Unterlagen ausschließlich über diese Vernichtungsgeräte zu entsorgen und nicht über den regulären Papiermüll. Die Vernichtung erfolgt zeitnah nach Wegfall der Aufbewahrungsnotwendigkeit.

c. **Physische Löschung von Datenträgern:** Nicht mehr benötigte Datenträger werden bei CTO vor einer Weitergabe oder Entsorgung physisch gelöscht, sodass eine Wiederherstellung der ehemals gespeicherten Daten ausgeschlossen ist. Je nach Datenträgertyp kommen geeignete Löschverfahren zum Einsatz, etwa mehrfaches Überschreiben oder eine physische Zerstörung des Datenträgers. Die Löschung bzw. Vernichtung wird dokumentiert. Dies gilt sowohl für interne Datenträger als auch für Datenträger, die im Rahmen der Auftragsverarbeitung eingesetzt wurden.

d. **Beauftragung eines externen, zertifizierten Aktenvernichters:** Größere Mengen an zu vernichtenden Unterlagen werden bei CTO über einen externen, spezialisierten Aktenver-

nichtungsdienstleister entsorgt. Die Vernichtung erfolgt gemäß den vertraglich vereinbarten Vorgaben und wird durch den Dienstleister entsprechend nachgewiesen. Der Transport der Unterlagen bis zur Vernichtung erfolgt durch den Dienstleister unter Beachtung angemessener Sicherheitsvorkehrungen. Auf Anfrage können entsprechende Vernichtungsnachweise vorgelegt werden. Für die laufende Entsorgung stehen zusätzlich in verschiedenen Bereichen Datenschutztonnen zur Verfügung, deren Inhalt durch zertifizierte Dienstleister nach den Vorgaben der DIN 66399 vernichtet wird.

18. Zutrittskontrolle (organisatorisch)

a. **Begleitung von Besuchern:** Besucher der CTO Balzuweit GmbH bewegen sich innerhalb der Geschäftsräume grundsätzlich nicht unbegleitet, sondern werden durchgehend von einem Mitarbeitenden begleitet. Dies gilt insbesondere für Bereiche, in denen vertrauliche Informationen oder personenbezogene Daten verarbeitet werden. Ein selbständiges Bewegen von Besuchern in solchen Bereichen ist ausgeschlossen. Die Begleitung endet erst mit dem Verlassen des Gebäudes durch den Besucher.

b. **Protokollierung von Besuchen:** Besuche werden bei CTO in einer Besucherliste protokolliert, die unter anderem Name, Ankunfts- und Abreisezeit sowie den Grund des Besuchs erfasst. Dies ermöglicht im Bedarfsfall eine Nachvollziehbarkeit, welche externen Personen sich zu welchem Zeitpunkt in den Geschäftsräumen aufgehalten haben. Die Erfassung erfolgt am Empfang bzw. Eingangsbereich. Die Besucherdaten werden unter Berücksichtigung der Aufbewahrungsfristen verarbeitet und anschließend gelöscht.

c. **Geregelte Schlüsselvergabe:** Die Ausgabe von Schlüsseln bzw. Zutrittsmedien zu den Geschäftsräumen der CTO Balzuweit GmbH erfolgt nach einem festgelegten Verfahren und wird dokumentiert. Es ist jederzeit nachvollziehbar, welche Person über welche Zutrittsberechtigung verfügt. Bei Verlust eines Schlüssels bzw. Zutrittsmediums oder beim Ausscheiden eines Mitarbeitenden erfolgt eine unverzügliche Sperrung bzw. Rückgabe. Die Schlüsselregelung wird regelmäßig überprüft.

d. **Sorgfältige Auswahl des Reinigungspersonals:** Reinigungsdienstleister, die Zugang zu den Geschäftsräumen der CTO Balzuweit GmbH erhalten, werden unter besonderer Sorgfalt ausgewählt und vertraglich zur Vertraulichkeit verpflichtet. Der Zutritt erfolgt in der Regel außerhalb der Kernarbeitszeiten und wird organisatorisch geregelt. Bei Bedarf wird der Zutritt zu besonders sensiblen Bereichen zusätzlich eingeschränkt oder beaufsichtigt. Die vertragliche Bindung stellt sicher, dass auch externes Reinigungspersonal den Vertraulichkeitsanforderungen von CTO unterliegt.

e. **Besetzter Empfang:** Der Empfang der CTO Balzuweit GmbH ist während der Geschäftszeiten durchgehend besetzt. Ankommende Besucher werden dort registriert und von dort in die jeweiligen Besprechungsräume begleitet. Dies ergänzt die Vorgabe, dass sich Besucher nicht unbegleitet im Gebäude bewegen.

f. **Zentrale Vergabe von Zutrittsberechtigungen:** Zutrittsberechtigungen zu den Geschäftsräumen der CTO Balzuweit GmbH werden zentral verwaltet und nur selektiv nach Freigabe durch die Geschäftsleitung vergeben. Eine pauschale oder automatische Vergabe von Zutrittsrechten findet nicht statt. Die vergebenen Berechtigungen werden regelmäßig überprüft.

g. **Differenzierte Sicherheitsbereiche:** Innerhalb der Geschäftsräume bestehen unterschiedliche Sicherheitsbereiche, etwa für Technikräume, die Geschäftsleitung, den Personalbereich und die IT. Diese Bereiche sind durch zusätzliche technische Maßnahmen gegenüber den allgemein zugänglichen Bürobereichen abgesichert. Der Zutritt ist auf einen entsprechend berechtigten Personenkreis beschränkt.

19. Zutrittskontrolle (technisch)

a. **Alarmanlage zur Gebäudesicherung:** Die Geschäftsräume und Eingänge der CTO Balzuweit GmbH sind durch eine Alarmanlage gesichert, die einen unbefugten Zutrittsversuch außerhalb der Geschäftszeiten erkennt und meldet. Überwacht werden hier speziell das EG (Lautlinger Weg 3) sowie der Serverraum im 1. OG. Im Alarmfall werden die zuständigen Stellen automatisiert informiert. Die Alarmanlage wird regelmäßig auf Funktionsfähigkeit geprüft und gewartet. Sie ergänzt die organisatorischen Zutrittsregelungen um eine technische Sicherungsebene.

b. **Elektronisches Zutrittskontrollsystem:** Die Geschäftsräume der CTO Balzuweit GmbH verfügen über ein elektronisches Zutrittskontrollsystem, das mit der Alarmanlage gekoppelt ist. Mitarbeitende erhalten einen personalisierten Zutrittstoken, über den ihnen Zutritt zu den jeweils benötigten Gebäuden und Räumen gewährt wird. Verlorene oder gestohlene Token werden umgehend gesperrt.

c. **Physische Sicherheit der Cloud-Infrastruktur:** CLARC-Cloud-Lösungen betreibt CTO ausschließlich bei Rechenzentrumsbetreibern mit gültiger Zertifizierung nach ISO/IEC 27001. Die physische Sicherung der Rechenzentren, einschließlich der Zutrittskontrolle vor Ort, liegt in der Verantwortung des jeweiligen zertifizierten Betreibers und wird im Rahmen der Auswahl und laufenden Bewertung von Unterauftragnehmern durch CTO berücksichtigt.

Datum: 20.08.2026

Markus Balzuweit
-Verantwortlicher-