Cloud Software Group Services Security Exhibit

Version 3.0

Gültig ab 30. September 2022

Inhalt

Dieses Cloud Software Group, Inc. („Cloud Software Group", „Wir", „Uns" oder „Unser") Services Security Exhibit (das „Exhibit") beschreibt die Sicherheitskontrollen, die in Verbindung mit der Ausführung von Cloud Services, technischen Support- oder Beratungsservices (die „Services") implementiert werden, die Kunden („Kunde", „Sie" oder „Ihr") im Rahmen der entsprechenden Cloud Services Group-Lizenz- und/oder Serviceleistungsvereinbarung und der entsprechenden Bestellung der Services (zusammenfassend die „Vereinbarung") zur Verfügung gestellt werden. Beta- oder Labor-/Technologievorschau-Services (einschließlich Cloud Labs) und unsere internen IT-Systeme, die nicht an der Bereitstellung von Services beteiligt sind, fallen nicht in den Geltungsbereich dieses Exhibit.

Begriffe in Großbuchstaben haben die in der Vereinbarung angegebene oder hierin definierte Bedeutung. „Kundeninhalte" sind alle Daten, auf die wir zugreifen oder die wir erhalten oder die Sie zur Speicherung oder Verarbeitung senden oder hochladen, damit wir die Services erbringen können. Dazu gehören auch geschützte technische Informationen, die mit Ihrer Umgebung verbunden sind, wie z. B. System- oder Netzwerkkonfigurationen und die von Ihnen gewählten Kontrollen.. „Protokolle" sind Informationen in Bezug auf Leistung, Stabilität, Nutzung, Sicherheit, Support, Hardware, Software, Services oder Peripheriegeräte, die mit der Nutzung unserer Produkte oder Services verbunden sind.

1. Geltungsbereich

Dieses Exibit beschreibt die administrativen, physischen und technischen Sicherheitskontrollen, die wir anwendet, um die Vertraulichkeit, Integrität und Verfügbarkeit unserer Services zu gewährleisten. Diese Kontrollen gelten für unsere Betriebs- und Servicesysteme und -umgebungen. Die Cloud Software Group verwendet ISO/IEC 27002 als Grundlage für ihr Sicherheitsprogramm für Services und hat Branchenzertifizierungen und Bewertungen für bestimmte Services erhalten. Weitere Informationen finden Sie im Abschnitt „Datenschutz und Compliance" in unserem Trust Center.

Wir sind bestrebt, seine Sicherheitspraktiken kontinuierlich zu verstärken und zu verbessern, und behält sich daher das Recht vor, die hier beschriebenen Kontrollen zu ändern. Jegliche Änderungen werden das Sicherheitsniveau während der betreffenden Laufzeit der Services nicht vermindern.

2. Sicherheitsprogramm und Richtlinien-Framework

Cloud Software Group verfügt über ein Sicherheitsprogramm und einen Rahmen für Sicherheitsrichtlinien, die von Führungskräften von, die verschiedene Geschäftsbereiche des Unternehmens repräsentieren, festgelegt und genehmigt wurden.

Übersicht über Sicherheitsrisiken

Das Cyber Risk Oversight Committee (CROC) regelt die Aktivitäten des Sicherheitsrisikomanagements. Das CROC besteht aus funktionsübergreifendem Führungskräften. Das Team aus Führungskräften überprüft die Mitgliedschaft in den Ausschüssen jährlich, um eine

angemessene Abdeckung der Geschäfts- und Betriebsbereiche zu bestätigen.

Das CROC tritt mindestens vierteljährlich zusammen und bietet Orientierungshilfen, Einblicke und Anweisungen zur Identifizierung, Bewertung und Behandlung von Sicherheitsrisiken sowohl in Unternehmen als auch in der Infrastruktur der Servicebereitstellung.

2.2 Verwaltung der Sicherheitsrisiken

Cloud Software Group setzt ein Programm zum Management von Sicherheitsrisiken (Security Risk Managment, SRM), das potenzielle Bedrohungen für unsere Produkte und Services sowie für unsere Infrastruktur identifiziert, die Bedeutung der mit diesen Bedrohungen verbundenen Risiken bewertet, Strategien zur Risikominderung entwickelt und mit unseren Produkt- und Entwicklungsteams zusammenarbeitet, um diese Strategien umzusetzen.

2.3 Informationssicherheit

Cloud Software Group hat einen Chief Information Security Officer (CISO) ernannt, der für die Sicherheitsaufsicht und die Strategie, Einhaltung und Durchsetzung von Richtlinien verantwortlich ist. Der Director of Security Monitoring and Response leitet den Reaktionprozess auf Sicherheitsvorfälle, einschließlich Untersuchung, Eindämmung und Behebung.

2.4 Physische und Umgebungssicherheit

Das Cloud Software Group Security-Team überwacht den physischen Zugang zu unseren Einrichtungen.

3. Zugangskontrolle

Wir verlangen den Einsatz von Zugangskontrollmaßnahmen, die sicherstellen sollen, dass für den Zugang auf Unternehmenssysteme, Vermögenswerte, Daten und Einrichtungen angemessene Privilegien zugewiesen und aufrecht erhalten werden, um vor potenziellen Schäden, Kompromittierungen oder Verlusten zu schützen. Wir folgen dem Least-Privilege-Prinzip oder der rollenbasierten Sicherheit, die den Zugang der Benutzer auf das beschränkt, was für die Ausführung von Aufgaben oder Rollen notwendig ist.

Manager entwerfen Rollen, um eine angemessene Aufgabentrennung zu gewährleisten, indem sie Aufgaben und Privilegien auf mehrere Personen verteilen, um sich vor Betrug und Fehlern zu schützen.

3.1 Neue Konten-, Rollen- und Zugriffsanfragen

Cloud Software Group schreibt eine formellen Anfragen für den Zugriff auf Unternehmenssysteme oder -daten vor. Jede Zugriffsanfrage erfordert eine Mindestgenehmigung durch den Vorgesetzten des Benutzers, um die Rolle und den Zugriff des Benutzers zu bestätigen. Zugriffsadministratoren bestätigen, dass vor der Gewährung des Zugriffs auf Systeme oder Daten die erforderlichen Genehmigungen angefordert wurden. Das Least-Privilege-Prinzip wird angewendet.

3.2 Kontoüberprüfung

Wir führen mindestens halbjährlich Überprüfungen von Benutzerkonten und zugewiesenen Berechtigungen für wichtige Systeme durch. Alle Änderungen, die als Ergebnis der Überprüfungen erforderlich sind, unterliegen einem formellen Zugriffsanfrageprozess, um den Benutzer zu bestätigen, und die Rolle des Benutzers erfordert Zugriff auf das/die entsprechenden System(e).

3.3 Entfernen von Konten, Rollen und Zugriffsrechten

Wir verlangen, dass der Benutzerzugriff unverzüglich nach der Benachrichtigung über die Änderung der Rolle eines Benutzers (falls zutreffend), die Kündigung, den Abschluss des Beschäftigungsverhältnisses eines Benutzers oder das Ausscheiden aus dem Unternehmen deaktiviert, widerrufen oder entfernt wird.

Anträge auf Entfernung des Zugriffs werden dokumentiert und verfolgt.

3.4 Anmeldeinformationen

Cloud Software Group verlangt eine mehrstufige Authentifizierung für den Remotezugriff von Mitarbeitern auf unsere Systeme und setzt die folgenden Verfahren zur Handhabung und Verwaltung von Kennwörtern durch:

- Kennwörter müssen regelmäßig gemäß den von uns festgelegten Systemanforderungen gewechselt werden.

- Kennwörter müssen die Anforderungen an Länge und Komplexität erfüllen, einschließlich einer Mischung aus Ziffern, Sonderzeichen und Groß- und Kleinbuchstaben, einer Mindestanzahl von Zeichen und dem Verbot von gebräuchlichen Wörtern oder Wörterbüchern.
- Deaktivierte oder abgelaufene Benutzer-IDs werden nicht an andere Personen vergeben.
- Wir verwenden Verfahren zur Deaktivierung von Kennwörtern an, die versehentlich weitergegeben wurden.
- Wir überwachen wiederholte Versuche, sich mit einem ungültigen Kennwort Zugriff auf Services zu verschaffen, und führt automatisierte Aktionen durch, um wiederholte Versuche zu blockieren.

Cloud Software Group wendet Praktiken an, die darauf ausgelegt sind, die Vertraulichkeit und Integrität von Kennwörtern bei deren Vergabe, Verteilung und Speicherung zu wahren, wie z. B:

- Anforderung, dass Kennwörter während ihres gesamten Lebenszyklus gehasht und/oder verschlüsselt bleiben
- Verbot der die gemeinsame Nutzung von Kennwörtern

4. Systementwicklung und -wartung

Wir verwenden einen „Secure by Design“-Prozess an, der Standards und Änderungskontrollverfahren umfasst, die auf die Sicherheitsanforderungen der Informationssysteme, die Überprüfung und das Testen des Codes und die Sicherheit bei der Verwendung von Testdaten ausgerichtet sind. Dieser Prozess wird von einem spezialisierten Sicherheitsteam geleitet und überwacht, das auch für die Überprüfung des Designs, die Bedrohungsmodellierung, die manuelle Codeüberprüfung und Stichproben sowie Penetrationstests zuständig ist.

4.1 Prinzipien für sicheres Design

Cloud Software Group hat eine formale Methodik für den Lebenszyklus der Systementwicklung (Systems Development Life Cycle, SDLC) eingeführt, die die Entwicklung, den Erwerb, die Implementierung und die Wartung von computergestützten Informationssystemen und die damit verbundenen technologischen Anforderungen regelt.

Wir verwenden ein softwarebasiertes System für die Verwaltung von Open-Source-Prüfungen und -Genehmigungen, wozu auch regelmäßige Scans und Audits seiner Softwareprodukte gehören. Wir verfügen über dokumentierte Richtlinien, die allen Mitarbeitern zur Verfügung stehen, bezüglich der Nutzung von Open Source sowie Schulungen für Entwickler und deren Management zu bewährten Open Source-Methoden.

4.2 Änderungsmanagement

Unser Änderungsmanagementprozess für Infrastruktur und Software richtet sich an Sicherheitsanforderungen und setzt voraus, dass Software- und Infrastrukturänderungen vor dem Einsatz in der Produktionsumgebung autorisiert, formal dokumentiert, getestet (falls zutreffend), überprüft und genehmigt werden. Infrastruktur- und Softwareänderungen werden mit Hilfe von Arbeitsverwaltungssystemen verwaltet und verfolgt.

Der Änderungsmanagementprozess ist angemessen getrennt, und der Zugang zur Migration von Änderungen in die Produktion ist auf autorisierte Mitarbeiter beschränkt.

5. Asset-Management

5.1 Physisches und virtuelle Asset-Management

Cloud Software Group unterhält ein dynamisches Inventar der von verwalteten physischen und virtuellen Systeme, die zur Erbringung der Services verwendet werden („Service-Assets“). Systemeigentümer sind für die Wartung und Aktualisierung ihrer Service-Assets in Übereinstimmung mit unseren Sicherheitsstandards verantwortlich.

Es gibt formelle Löschverfahren, die das sichere Löschen von Cloud Software Group- und Kundendaten regeln. Wir löschen Daten, wenn sie nicht mehr benötigt werden, auf der Grundlage einer Klassifizierung und unter Verwendung von Löschprozessen, die verhindern sollen, dass Daten rekonstruiert oder gelesen werden können.

Unsere technologischen Assets werden bereinigt und gelöscht, wenn sie in dem ihnen zugewiesenen oder zugewiesenen Bereich nicht mehr benötigt werden. Zu den technologischen Asstes gehören unter anderem einzelne Computergeräte, Multifunktions-Computergeräte, Speichergeräte, Bildgebungsgeräte und Netzwerkgeräte. Die Entsorgung wird durch Services für globale Sicherheitsrisiken und Informationssicherheit koordiniert.

5.2 Anwendungs- und Systemmanagement

Anwendungs- und Systemeigentümer sind verantwortlich für die Überprüfung und Klassifizierung der Daten, die sie speichern, auf die sie zugreifen, über die sie verfügen oder die sie übertragen. Neben anderen Kontrollen sind Mitarbeiter und Auftragnehmer zu Folgendem verpflichtet:

- Einstufen von Kundeninhalten als eine der beiden höchsten Kategorien vertraulicher Citrix Informationen und Anwendung entsprechender Zugriffsbeschränkungen
- Drucken von Kundeninhalten beschränken und gedruckte Materialien in sicheren Behältern entsorgen
- Unternehmens- oder vertrauliche Informationen nicht auf Geräten speichern, die nicht den Anforderungen der Sicherheitsrichtlinien und -standards von Citrix entsprechen
- Unbeaufsichtigte Computer und Daten sichern

5.3 Aufbewahrung von Daten

Kundeninhalte, die als Teil unserer Cloud Services gespeichert sind, sind für einen begrenzten Zeitraum nach der Beendigung der Services für den Kunden zugänglich und werden dann (mit Ausnahme von Sicherungskopien) gelöscht, nachdem der Kunde eine Bestätigung über die Löschung erhalten hat. Weitere Einzelheiten sind in der Dokumentation zu den einzelnen Services aufgeführt. Kundeninhalte können auch nach Erbringung der Services beibehalten werden, wenn dies aus rechtlichen Gründen erforderlich ist. Citrix wird die Anforderungen dieses Exibits erfüllen, bis diese Kundeninhalte endgültig gelöscht wurden.

6. Sicherheit für die Personalabteilung

Die Aufrechterhaltung der Sicherheit von Kundeninhalten ist eine der Kernanforderungen für alle Mitarbeiter und Auftragnehmer. Unser Code of Business Conduct verlangt von allen Mitarbeitern und Auftragnehmern die Einhaltung unserer Sicherheitsrichtlinien und -standards und zielt insbesondere auf den Schutz vertraulicher Informationen sowie persönlicher Daten von Kunden, Partnern, Lieferanten und Mitarbeitern ab.

Alle Mitarbeiter und Auftragnehmer unterliegen

Vertraulichkeitsvereinbarungen, die sich auf Kundeninformationen beziehen. Die Cloud Software Group Security-Organisation kommuniziert auch regelmäßig mit den Mitarbeitern über Themen der Informations- und physischen Sicherheit, um das Sicherheitsbewusstsein für bestimmte Themen aufrechtzuerhalten.

6.1 Background-Checks

Wir bedienen uns derzeit bei allen Neueinstellungen weltweit der Anbieter von Background-Checks und verlangen das Gleiche für das Personal von Drittanbietern, es sei denn, dies ist durch örtliche Gesetze oder arbeitsrechtliche Bestimmungen eingeschränkt.

6.2 Schulung

Alle Mitarbeiter sind verpflichtet, Schulungen zum Datenschutz und zu den Unternehmensrichtlinien zum Schutz der Sicherheit unserer vertraulichen Informationen zu absolvieren, wozu auch die vertraulichen Informationen unserer Kunden, Partner, Lieferanten und Mitarbeiter gehören. Die Schulungen befassen sich mit den Datenschutzpraktiken und den Prinzipien, die für den Umgang von Mitarbeitern mit persönlichen Daten gelten, einschließlich der Notwendigkeit, Einschränkungen für die Nutzung, den Zugriff, die Weitergabe und die Aufbewahrung persönlicher Daten festzulegen. Mitglieder der Abteilung Engineering durchlaufen eine spezifische Schulung mit den Themen Entwicklung, Architektur und Codierung.

6.3 Durchsetzung

Alle Mitarbeiter sind verpflichtet, unsere Sicherheits- und Datenschutzrichtlinien und -standards einzuhalten. Bei Nichteinhaltung drohen Disziplinarmaßnahmen bis hin zur Kündigung des Arbeitsverhältnisses.

7. Betriebliche Sicherheit

7.1 Netzwerk- und Systemsicherheit

Cloud Software Group verfügt über dokumentierte Standards zur Netzwerk- und Systemhärtung, die sicherstellen sollen, dass Netzwerke und Systeme sicher konfiguriert werden. Zu den nach diesen Standards erforderlichen Verfahren gehören unter anderem:

- Ändern oder Deaktivieren von Standardeinstellungen und/oder Konten
- Kontrollierte Nutzung des administrativen Zugangs
- Einschränken von Servicekonten nur für den Zweck, für den sie erstellt wurden
- Konfigurieren geeigneter Protokollierungs- und Alarmeinstellungen für Audits

Wir verlangent die Implementierung von Anti-Malware-Software auf Servern und Arbeitsstationen und scannen das Netzwerk nach bösartiger Software.

Netzwerkkontrollen regeln den Zugriff auf Kundeninhalte. Dazu gehören gegebenenfalls: die Konfiguration einer nicht vertrauenswürdigen Zwischenzone zwischen dem Internet und dem internen Netzwerk, die einen Sicherheitsmechanismus zur Beschränkung des Zugriffs und des nicht autorisierten Datenverkehrs enthält; die Segmentierung des Netzwerks, um den nicht autorisierten Zugriff auf Kundeninhalte zu verhindern; und die Trennung von Web- und Anwendungsservern von den entsprechenden Datenbankservern in einer abgestuften Struktur, die den Verkehr zwischen den Schichten einschränkt.

7.2 Protokollierung

Wir sammeln Protokolle, um das korrekte Funktionieren seiner Services zu bestätigen, bei der Fehlerbehebung von Systemproblemen zu helfen und seine Netzwerke und Kundeninhalte zu schützen und zu sichern. Protokolle können Zugriffs-ID, Zeit, gewährte oder verweigerte Autorisierung, Diagnosedaten wie Ablaufverfolgungs- und Absturzdateien sowie andere relevante Informationen und Aktivitäten enthalten.

Wir erfassen und verwenden Protokolle (i) für die Bereitstellung, Sicherung, Verwaltung, Messung und Verbesserung der Services, (ii) auf Anfrage des Kunden oder seiner Endbenutzer, (iii) für die Rechnungsstellung, Kontoverwaltung, interne Berichterstattung und Produktstrategie und/oder (iv) zur Einhaltung von Vereinbarungen, Richtlinien, geltenden Gesetzen, Vorschriften oder behördlichen Anforderungen. Dazu kann die Überwachung der Leistung, Stabilität, Nutzung und Sicherheit der Services und der damit verbundenen Komponenten gehören. Protokolle können Zugriffs-ID, Zeit, gewährte oder verweigerte Autorisierung, Diagnosedaten wie Ablaufverfolgungs- und Absturzdateien sowie andere relevante Informationen und Aktivitäten enthalten. Kunden dürfen diese Überwachung nicht blockieren oder stören.

Weitere Informationen zum Umgang mit Kundeninhalten und Protokollen finden Sie in unserem Trust Center Cloud Assurance Data Protection & Security section, das mehrere Whitepaper zur Protokollierung von Citrix Cloud Services enthält.

7.3 Verwaltung von Zertifikaten, Anmeldeinformationen und Geheimnissen

Die Cloud Software Group unterhält Richtlinien, die den Lebenszyklus von Zertifikaten, Anmeldeinformationen und Geheimnissen abdecken, um Schutz, Verfügbarkeit und Vertraulichkeit zu gewährleisten. Geheimnisträger müssen dokumentiert werden und förmlich bestätigen, dass sie die Verantwortung als Geheimnisträger übernehmen.

Zu den Aufgaben gehören unter anderem:

- Die Zertifikate müssen von einer zugelassenen Zertifizierungsstelle ausgestellt werden.
- Kryptografische Schlüssel dürfen nicht im Klartext gespeichert oder übertragen werden und müssen starke, anerkannte kryptografische Protokolle verwenden.
- Anmeldeinformationen und Geheimnisse müssen mindestens einmal pro Jahr erneuert und in einem zugelassenen Tool zur Verwaltung privilegierter Authentifizierung gespeichert werden.

7.4 Schwachstellenmanagement

Wir überwachen Anwendungen und Systeme regelmäßig mit automatischen Schwachstellen- und Port-Scans auf Schwachstellen.

Ermittelte Schwachstellen müssen nach einem Zeitplan behoben werden, der vom Schweregrad und den Empfehlungen des Anbieters abhängt. In Fällen, in denen kein Patch, Update oder eine dauerhafte Lösung verfügbar ist, werden geeignete Gegenmaßnahmen ergriffen, um das Risiko der Ausnutzung der Schwachstelle zu verringern.

8. Verschlüsselung

8.1 Schutz bei der Datenübertragung

Cloud Software Group hat sichere Übertragungsprotokolle für die Übertragung von Daten über öffentliche Netzwerke eingesetzt, die Teil der Services sind. Die Services sind durch Verschlüsselung geschützt, und der Zugriff über das Internet ist durch TLS-Verbindungen geschützt.

8.2 Schutz von Daten im Ruhezustand

Wir verlangen, dass alle Arbeitsstationen, die für die Bereitstellung von Services verwendet werden, mit mindestens 128-Bit-Festplattenverschlüsselung verschlüsselt sind. Kundeninhalte dürfen nicht auf einem tragbaren Gerät gespeichert werden, es sei denn, sie sind verschlüsselt.

Einige Cloud Services verschlüsseln bestimmte Datenelemente standardmäßig und können auch andere Verschlüsselungsfunktionen anbieten, die der Kunde implementieren kann. Weitere Einzelheiten entnehmen Sie bitte der entsprechenden Dokumentation zu den Cloud Services.

9. Physische Sicherheit

9.1 Einrichtungen

Wir haben die folgenden Kontrollen implementiert, die den unbefugten Zugang zu allen Einrichtungen verhindern sollen:

- Der Zugang zu den Einrichtungen ist auf autorisierte Personen beschränkt.
- Besucher müssen sich in eine digitale Besucherliste eintragen und müssen jederzeit begleitet oder beobachtet werden.
- Ausweiskarten sind für Mitarbeiter, Auftragnehmer und Gäste erforderlich und müssen jederzeit sichtbar sein, wenn sie sich in der Einrichtung befinden.
- Die Sicherheitsabteilung verwaltet und kontrolliert den Zugang zu den Einrichtungen nach Betriebsschluss.
- Wachleute, Einbruchserkennung und/oder CCTV-Kameras überwachen Gebäudeeingangspunkte, Lade- und Versanddocks und öffentliche Zugangsbereiche (die Mechanismen zur Überwachung des Zugangs können je nach Einrichtung und Standort unterschiedlich sein).

Darüber hinaus bieten die Einrichtungen der Cloud Software Group Folgendes:

- Feuerunterdrückungs- und Feuererkennungssysteme oder -vorrichtungen
- Klimaregelungssysteme oder -geräte (Temperatur, Feuchtigkeit usw.)
- Zugängliches Hauptabsperrventil oder Absperrventil für Wasser
- Notausgänge und Evakuierungswege

Datenschränke, die sich in Büros befinden, sind durch Zugang per Ausweis geschützt.

9.2 Datencenter

Zusätzlich zu den oben beschriebenen Einrichtungskontrollen für Cloud Software Group-eigene und verwaltete Einrichtungen führen wir zusätzliche Kontrollen in den Datencentern ein, die zur Bereitstellung von Services genutzt werden.

Wir verwenden Systeme zum Schutz vor Datenverlusten aufgrund von Stromversorgungsausfällen oder Leitungsstörungen, einschließlich einer globalen und redundanten Service-Infrastruktur, die mit Standorten für die Notfallwiederherstellung eingerichtet ist. Datencenter und Internetdienstanbieter (Internet Service Providers, ISPs) werden evaluiert, um die Leistung in Bezug auf Bandbreite, Latenz und Isolierung der Notfallwiederherstellung zu optimieren.

Datencenter befinden sich in Einrichtungen, die ISP-Träger-neutral sind und physische Sicherheit, redundante Stromversorgung, Infrastruktur-Redundanz und Betriebszeitvereinbarungen von wichtigen Lieferanten bieten.

Wenn wir für die Bereitstellung der Services Datencenter Dritter oder Cloud

Services nutzen, beauftragen wir Anbieter, die die physischen und umgebungsbedingten Sicherheitsanforderungen unserer Einrichtungen erfüllen oder übertreffen.

10. Business Continuity und Disaster Recovery

10.1 Business Continuity

Cloud Software Group plant strategisch für die Fortführung des Geschäftsbetriebs in ungünstigen oder störenden Situationen und entwirft Systeme, damit die Services während des Auftretens solcher Ereignisse funktionsfähig bleiben.

Wir führen mindestens alle zwei Jahre eine Business Impact Analysis (BIA) auf Abteilungsebene durch, mit einer jährlichen Überprüfung jedes Jahr. Die BIA wird zur Erstellung eines abteilungsbezogenen Geschäftskontinuitätsplans (Business Continuity Plan, BCP) verwendet, der für jede Abteilung deren Ressourcenbedarf, Wiederherstellungsparameter und -methoden, Umzugsanforderungen und die während des gesamten Prozesses erforderlichen Sicherheitsmaßnahmen zur Vermeidung von Ausfällen oder Lücken identifiziert und dokumentiert. Der Leiter jeder Abteilung überprüft und genehmigt den BCP jährlich oder bei wichtigen organisatorischen Änderungen.

Wir verfügen über Notfall- und Notfallpläne für alle unsere Einrichtungen. Für den Fall, dass die Einrichtungen nicht verfügbar sind, haben die Mitarbeiter die Möglichkeit, entweder in anderen Cloud Software Group-Einrichtungen oder an einem Ort ihrer Wahl von einem Remotestandort aus zu arbeiten. Zusätzliche Wiederherstellungsstrategien werden gegebenenfalls in den BCPs dokumentiert.

10.2 Disaster Recovery

Wir sind bestrebt, die Auswirkungen von Service- oder Betriebsunterbrechungen zu minimieren, indem Prozesse und Kontrollen implementiert werden, die eine stabile und ordnungsgemäße Wiederherstellung sowie eine Wiederherstellung der unserer Geschäftssysteme und -daten gewährleisten. Cloud Software Group implementiert Redundanz für alle unternehmenskritischen Systeme, Daten und Infrastruktur. Der Notfallwiederherstellungsplan (Disaster Recovery Plan, DRP) nutzt die in der oben erwähnten BIA durchgeführte Bewertung, um Parameter, Methoden, Prioritäten und Sicherheitsvorkehrungen für die Wiederherstellungszeit zu identifizieren und zu dokumentieren, die während des gesamten Prozesses erforderlich sind, um Ausfälle oder Lücken zu vermeiden.

Der Plan skizziert die Gesamtstruktur und den Ansatz zur Wiederherstellung kritischer Systeme und Daten, einschließlich, aber nicht beschränkt auf die Wiederherstellung:

- Rollen und Verantwortlichkeiten von Einzelpersonen oder Teams
- Kontaktinformationen für wichtiges Personal oder Drittparteien
- Schulungsanforderungen und -pläne für wichtiges Personal
- Wiederherstellungsziele, Wiederherstellungsprioritäten und Erfolgsmetriken
- Schema der vollständigen Wiederherstellung

Der Leiter überprüft und genehmigt den DRP jährlich oder bei wichtigen organisatorischen Änderungen.

11. Reaktion auf Sicherheitsvorfälle

Cloud Software Group verwendet einen Cyber Security Incident Response Plan (Reaktionsplan für Cyber-Sicherheitsvorfälle), der die Prozesse zur Erkennung, Meldung, Identifizierung, Analyse und Reaktion auf Sicherheitsvorfälle mit Auswirkungen auf von uns verwaltete Netzwerke und/oder Systeme oder Kundeninhalte detailliert beschreibt. Schulungen zur Reaktion auf Sicherheitsvorfälle und Tests finden mindestens jährlich statt.

„Sicherheitsvorfall“ bedeutet unbefugten Zugriff auf Kundeninhalte, der zum Verlust der Vertraulichkeit, Integrität oder Verfügbarkeit führt. Wenn wir feststellen, dass Kundeninhalte, die sich in unserer Kontrolle befinden, Gegenstand eines Sicherheitsvorfalls waren, wird der Kunde innerhalb der gesetzlich vorgeschriebenen Frist benachrichtigt. Unsere Mitteilung beschreibt, soweit bekannt, die Art des Vorfalls, den Zeitraum und die potenziellen Auswirkungen auf den Kunden.

Wir führen über jeden Sicherheitsvorfall eine Aufzeichnung.

12. Lieferantenverwaltung

Cloud Software Group kann Subunternehmer und Vertreter beauftragen, Services bereitzustellen. Alle Subunternehmer und Vertreter sind nur dann zum Zugriff auf Kundeninhalte berechtigt, wenn dies zur Erbringung der Services erforderlich ist, und sind an schriftliche Vereinbarungen gebunden, die sie dazu verpflichten, mindestens das Datenschutzniveau zu gewährleisten, das von uns durch diese Ausstellung gefordert wird. Wir bleiben zu jeder Zeit für die Einhaltung der Bestimmungen der Vereinbarung durch seine Subunternehmer und Vertreter verantwortlich. Eine Liste der Unterauftragsverarbeiter der Cloud Software Group, die Zugang zu den Kundeninhalten haben können, ist unter Unser Trust Center verfügbar.

12.1 Onboarding

Das Third-Party Risk Management-Programm (Risikomanagement-Programm für Dritte) von Citrix bietet einen systematischen Ansatz für das Management von Sicherheitsrisiken, die durch den Einsatz von Drittanbietern entstehen. Wir arbeiten daran, Sicherheitsrisiken zu identifizieren, zu analysieren und zu mindern, bevor es zu einer Beteiligung von Dritten kommt.

Cloud Software Group schließt Vereinbarungen mit Lieferanten ab, um relevante Sicherheitsmaßnahmen und -verpflichtungen zu dokumentieren, die mit den in diesem Anhang aufgeführten übereinstimmen.

12.2 Fortlaufende Bewertung

Wir führen in regelmäßigen Abständen Sicherheitsrisikobewertungen durch, um sicherzustellen, dass die Sicherheitsmaßnahmen während der gesamten Lieferantenbeziehung angewendet werden. Änderungen der erbrachten Services oder Änderungen bestehender Verträge erfordern eine Bewertung des Sicherheitsrisikos, um zu bestätigen, dass die Änderungen kein zusätzliches oder unangemessenes Risiko darstellen.

12.3 Offboarding

Wir bemühen uns, die Beschaffungsabteilung des Unternehmens mindestens 90 Tage vor der geplanten Beendigung einer Lieferantenbeziehung oder vor dem Auslaufen eines Vertrags mit einem Lieferanten zu benachrichtigen (es sei denn, eine frühere Kündigung ist erforderlich). Die Beschaffungsabteilung des

Unternehmens koordiniert die Beendigung der bestehenden Beziehungen, um zu bestätigen, dass die unsere Unternehmensdaten und Assets gesichert und ordnungsgemäß behandelt werden.

13. Compliance

13.1 Umgang mit personenbezogenen Daten

Personenbezogene Daten sind Informationen, die sich auf eine identifizierte oder identifizierbare Person beziehen. Sie legen die personenbezogenen Daten fest, die in die Kundeninhalte aufgenommen werden sollen. Bei der Bereitstellung der Services fungieren wir als Datenverarbeiter, und Sie bleiben der Datenverantwortliche für alle in den Kundeninhalten enthaltenen personenbezogenen Daten. Wir werden auf Ihre Anweisung hin bezüglich der Verarbeitung solcher personenbezogener Daten handeln, wie in der Vereinbarung festgelegt.

Weitere Informationen zur Verarbeitung personenbezogener Daten, die der Datenschutz-Grundverordnung unterliegen, einschließlich der Mechanismen, die für den internationalen Transfer solcher Daten verwendet werden, werden in der Cloud Software Group Nachtrag zur Datenverarbeitung bereitgestellt.

13.2 Standort der Services

Die Kunden von Cloud Services behalten die Kontrolle über die Wahl des geografischen Standorts ihrer Cloud Services. Zu keinem Zeitpunkt während des geltenden Cloud Services-Abonnements werden wir den geografischen Standort der von Ihnen gewählten Umgebung ohne Ihre Zustimmung ändern. Beachten Sie, dass bei einigen Cloud Services die Auswahl bestimmter geografischer Standorte nicht möglich ist und dass im Rahmen der allgemeinen Service-Bereitstellung Kundeninhalte in die Vereinigten Staaten oder andere Länder übertragen werden können, in denen Citrix und/oder seine Serviceanbieter tätig sind, soweit dies für die Bereitstellung der Services erforderlich ist.

13.3 Offenlegung von Kundeninhalten

Wir dürfen Kundeninhalte in dem gesetzlich vorgeschriebenen Umfang offenlegen, einschließlich als Reaktion auf eine Vorladung, gerichtliche oder behördliche Anordnung oder ein anderes bindendes Instrument (jeweils eine „Forderung“). Außer in Fällen, in denen dies gesetzlich verboten ist, werden wir Sie unverzüglich über jede Anforderung informieren und Ihnen die Unterstützung zukommen lassen, die vernünftigerweise erforderlich ist, damit Sie rechtzeitig auf die Anforderung reagieren können.

13.4 Kundensicherheit und gesetzliche Anforderungen

Die Services sind so konzipiert, dass sie innerhalb einer größeren IT-Umgebung des Kunden bereitgestellt werden. Daher tragen die Kunden die volle Verantwortung für alle Sicherheitsaspekte, die nicht ausdrücklich von Citrix verwaltet werden, einschließlich, aber nicht beschränkt auf die technische Integration mit den Services, die Benutzerzugriffsverwaltung und -kontrolle sowie alle Anwendungen und Netzwerke, die die Kunden in Verbindung mit den Services nutzen.

Sie bleiben dafür verantwortlich, zu bestimmen, ob Ihre Nutzung der Services, einschließlich der Gewährung des Zugriffs auf Kundeninhalte als Teil der Services, über die in der Vereinbarung, einschließlich dieses Exhibit, festgelegten Anforderungen hinausgehenden gesetzlichen Bestimmungen oder

Sicherheitsanforderungen unterliegt. Kunden müssen daher sicherstellen, dass sie keine Kundeninhalte einsenden oder speichern, die Gesetzen unterliegen, die spezifische Kontrollen vorschreiben, die nicht in dieser Ausstellung enthalten sind, wie z. B. die US International Traffic in Arms Regulations (ITAR) oder ähnliche Bestimmungen eines Landes, das den Import oder Export von Verteidigungsartikeln oder Verteidigungsdienstleistungen einschränkt, geschützte Gesundheitsinformationen („PHI“), Zahlungskarteninformationen („PCI“) oder Daten für den kontrollierten Vertrieb gemäß Regierungsvorschriften, es sei denn, dies ist in der Vereinbarung und der anwendbaren Servicebeschreibung angegeben und die Parteien haben im Voraus zusätzliche Vereinbarungen (wie z. B. ein HIPAA Business Associate Agreement) getroffen, die für die Verarbeitung solcher Daten durch uns erforderlich sind.

14. Kundenaudits und -anfragen

Bis zu einmal jährlich wird Cloud Software Group auf Audit-Anfragen in Form von Antworten auf Risikobewertungen der Kunden antworten. Kunden können auch jederzeit auf unser Due Diligence Package zugreifen, um ein aktualisiertes Sicherheitspaket und einen aktualisierten Fragebogen zu erhalten. Unser Due Diligence Package wurde für Kundensicherheitsabfragen erstellt und stellt jederzeit verfügbare Sicherheitsinformationen bereit, einschließlich eines ausgefüllten Standardized Information Gathering (SIG) Lite-Fragebogens von Shared Assessments für unsere Cloud Services. Das Due Diligence Package kann über unser Trust Center in Abschnitt „Datenschutz und Sicherheit für Cloud Assurance“ heruntergeladen werden.

15. Kontakte

Funktion	Kontakt
Kundensupport	https://www.citrix.com/contact/technical-support.html
Melden eines Sicherheitsvorfalls	secure@citrix.com
Mutmaßliche Schwachstellen in unseren Services	https://www.citrix.com/about/trust-center/ (Klicken Sie auf die Schaltfläche „Sicherheitsvorfall melden“).

Enterprise Sales

Nordamerika | 800-424-8749
Weltweit | +1 408-790-8000

Standorte

Hauptsitz des Unternehmens | 851 Cypress Creek Road Fort Lauderdale, FL 33309, Vereinigte Staaten Silicon Valley | 4988 Great America Parkway Santa Clara, CA 95054, Vereinigte Staaten