Informationssicherheitsrichtlinie (öffentliche Version)

Einleitung

Bei COCUS legen wir großen Wert auf den Schutz von Informationen und die Einhaltung höchster Standards in Bezug auf Sicherheit, Datenschutz und Geschäftskontinuität. Unser Engagement gewährleistet die Vertraulichkeit, Integrität und Verfügbarkeit aller Systeme und Daten, die sowohl für unseren Betrieb als auch für unsere Kunden von entscheidender Bedeutung sind.
Wir verbessern kontinuierlich unser Informationssicherheitsmanagementsystem (ISMS) und unsere Prozesse, implementieren robuste Sicherheitskontrollen und -technologien und investieren in die Schulung und Sensibilisierung unserer Mitarbeiter.
Das COCUS-Engagement bezieht die gesamte Organisation ein, wobei die Geschäftsleitung die Verantwortung für die Kommunikation und Umsetzung übernimmt und sich verpflichtet, mit dem Fokus auf die Erreichung der festgelegten Ziele zu handeln.
Dieses Dokument beschreibt den COCUS-Ansatz zum Schutz von Daten und zur Einhaltung internationaler Standards und Best Practices und hebt die Hauptkomponenten unserer Informationssicherheitsrichtlinien hervor.

Organisatorische Sicherheit

Engagierte Teams:
Bei COCUS haben wir drei Teams, die sich der Informationssicherheit und dem Datenschutz widmen:

- Das Informationssicherheitsteam ist verantwortlich für Governance, Risiken, Compliance, die zweite Verteidigungslinie, das Managementsystem und das allgemeine Sicherheits- und Business Continuity-Programmmanagement.

- Das Datenschutzteam ist dafür verantwortlich, die Einhaltung der Datenschutzgesetze und -vorschriften sicherzustellen, die für COCUS als Verantwortlicher und/oder Auftragsverarbeiter gelten.

- Das IT-Team für sichere Operationen. Sie ist verantwortlich für das Vulnerability Management, die Incident Detection und Response, das Monitoring, die Identitäts-

und Zugriffskontrolle, die Resilienz und die Umsetzung der definierten Maßnahmen zur Business Continuity.

Integriertes Managementsystem:

COCUS verfügt über ein integriertes Managementsystem, das auf Folgendes ausgerichtet ist:

- TISAX- und ISO 27001-Standards für Informationssicherheitsmanagementsysteme (ISMS).

Unser Managementsystem umfasst Richtlinien, Anweisungen und Standards, die einen systematischen Ansatz zum Schutz von Unternehmensinformationen und -ressourcen bieten sollen. Dieser Ansatz gewährleistet einen Schutz, der auf der Kritikalität und Sensibilität von Informationen basiert, interne und externe Bedrohungen mindert und das Risiko auf ein akzeptables Maß reduziert.

Diese Richtlinien gelten für alle Mitarbeiter und anderes Personal. Sie werden mindestens einmal jährlich überprüft und decken mehrere Bereiche im Zusammenhang mit Sicherheit und Datenschutz ab, darunter Governance, Risikomanagement, Incident Management, Personalsicherheit, Management von Drittanbietern, Datenschutzmanagement und andere.

Das Informationssicherheitsteam ist für die Überwachung der Einhaltung der oben genannten Richtlinien, Anweisungen und Standards verantwortlich.

Klassifizierung von Informationen

COCUS hat einen Prozess zur Klassifizierung von Informationen implementiert, um sicherzustellen, dass Daten auf der Grundlage ihrer Sensibilität angemessen identifiziert, gehandhabt und geschützt werden, wodurch Risiken reduziert und die Vertraulichkeit, Integrität und Verfügbarkeit von Informationen gewahrt werden.

Vertraulichkeitsvereinbarungen

COCUS verlangt von Partnern, Dienstleistern und Mitarbeitern, dass sie Geheimhaltungs- und Vertraulichkeitsvereinbarungen unterzeichnen, um sicherzustellen, dass sie sich an die Informationssicherheitsprinzipien des Unternehmens halten.

Sicherheit der Humanressourcen

Personen, die sich mit COCUS-Systemen verbinden, müssen sich an die Sicherheitsrichtlinien des Unternehmens halten. Dazu gehören auch Verantwortlichkeiten während und nach der Beschäftigung bei COCUS.

Verhaltenskodex

Der Verhaltenskodex und die interne Regelung von COCUS befassen sich mit der angemessenen Verwendung von Informationen durch das Unternehmensmanagement, zu denen die Mitarbeiter während der Ausführung der Arbeitsvereinbarung mit COCUS

Zugang haben. Verstöße gegen den Kodex oder die Unternehmensrichtlinien werden in Übereinstimmung mit den lokalen Arbeitsgesetzen einem Disziplinarverfahren unterzogen.

Schulungen und Sensibilisierung für Sicherheit und Datenschutz

COCUS bietet ein Schulungs- und Sensibilisierungsprogramm für Sicherheit und Datenschutz an, das Folgendes umfasst:

- Die Mitarbeiter von COCUS werden im Rahmen des Onboarding-Prozesses in den Bereichen Sicherheit und Datenschutz geschult.
- COCUS bietet regelmäßige Schulungen und Sensibilisierungen an, um die Sicherheits- und Datenschutzprinzipien und -richtlinien sowie die Best Practices der Branche und häufige Fallstricke zu stärken.
- COCUS bietet gezielte Schulungen und Sensibilisierung an, um sicherzustellen, dass die Rollen, die aufgrund ihrer Verantwortlichkeiten, Zugriffsebenen und Funktionen ein Risiko für COCUS darstellen können, die richtige Schulung erhalten.

Darüber hinaus verteilt das Informationssicherheitsteam bei Bedarf unternehmensweite Sicherheitswarnungen.

Offboarding-Prozesse

COCUS verfügt über einen definierten Offboarding-Prozess, der die Verantwortlichkeiten für das Sammeln von Informationsbeständen und den Entzug von Zugriffsrechten für Mitarbeiter, die unser Unternehmen verlassen, umreißt.

COCUS hat Richtlinien und Standards eingeführt und umgesetzt, um die Sicherheit der Infrastruktur, die physische Sicherheit und den sicheren Betrieb zu gewährleisten. Dazu gehören wichtige Richtlinien wie Identitäts- und Zugriffsmanagement, Passwortverwaltung, Risikomanagement, Incidentmanagement, Änderungsmanagement, Verwaltung von Drittanbietern, Audit-Management und mehr. Alle Richtlinien und zugehörigen Dokumente wurden in Übereinstimmung mit den Anforderungen von TISAX und ISO 27001 sowie den Best Practices der Branche entwickelt und gepflegt.
COCUS hat mehrere Anforderungen in Bezug auf die Verschlüsselung von Daten, die Komplexität von Passwörtern und das Passwort-Manager-System, Authentifizierungsmechanismen, Endpunktsicherheit, Ereignisprotokollierung und Auditing implementiert.
Für weitere Informationen über unser Informationssicherheitsmanagementsystem (ISMS) und die damit verbundenen Richtlinien wenden Sie sich bitte an unser Team.

Physische Sicherheit

Der Zugang zu den COCUS-Einrichtungen ist auf autorisierte Mitarbeiter und Auftragnehmer beschränkt. COCUS implementierte einen Ansatz zur Einteilung von Sicherheitszonen mit spezifischen organisatorischen und technischen Sicherheitsvorkehrungen für Bereiche, die einen hohen Schutzbedarf erfordern.

Sicherheitsoperationen

Schwachstellen-Management
Die engagierten Teams von COCUS identifizieren, bewerten und beheben regelmäßig Sicherheitslücken durch Patches und Updates.

Patch-Management
COCUS hat einen Patch-Management-Prozess implementiert, um sicherzustellen, dass Systeme und Infrastruktursysteme gemäß den Empfehlungen des Anbieters gepatcht werden.
Der Prozess umfasst Schritte zur Überprüfung vorgeschlagener Patches, um das Risiko der Anwendung oder Nichtanwendung von Patches zu bestimmen, basierend auf den Auswirkungen auf Sicherheit und Verfügbarkeit dieser Systeme und aller kritischen Anwendungen, die auf ihnen gehostet werden. COCUS überprüft, patcht und aktualisiert, sobald sie veröffentlicht werden, um ihre Kritikalität zu bestimmen.

Penetrationstests
Unabhängige Penetrationstests werden durchgeführt, um die Sicherheitslage eines Zielsystems oder einer Zielumgebung zu bewerten. Diese Tests folgen einer anerkannten branchenüblichen Methodik.

Veränderungsmanagement
Das Ziel des COCUS-Change-Management-Prozesses ist es, ungeplante Serviceunterbrechungen zu verhindern und die Integrität der für die Kunden erbrachten Services zu wahren. Daher werden alle Änderungen vor der Bereitstellung überprüft, getestet und genehmigt.

Trennung der Aufgaben
Die Verantwortlichkeiten sind innerhalb von COCUS klar getrennt, um Möglichkeiten für unbefugte oder unbeabsichtigte Änderungen an Infrastruktur oder Systemen zu reduzieren.

Asset-Verwaltung

COCUS verwendet eine Asset-Management-Lösung, um alle mobilen Geräte zu verwalten und die Geräteeinrichtung, Updates für Apps und Betriebssysteme sowie Sicherheitsprotokolle zu automatisieren.

Backups

Regelmäßige Backups werden durchgeführt und getestet, um die Zuverlässigkeit zu gewährleisten. Die Häufigkeit der Backups richtet sich nach unseren Anforderungen an die Analyse der Auswirkungen auf das Geschäft und die Notfallwiederherstellung.

Endpunkt-Sicherheit

COCUS hat Endpoint Security-Maßnahmen implementiert, um mobile Geräte und Server vor Cyberbedrohungen zu schützen und eine sichere und geschützte Umgebung über alle Endpunkte hinweg zu gewährleisten.

Management von Incidents

COCUS verfolgt eine robuste Incident-Management-Richtlinie und -Verfahren für Ereignisse und Vorfälle, die die Vertraulichkeit, Integrität oder Verfügbarkeit von Systemen oder Daten beeinträchtigen oder möglicherweise gegen COCUS-Richtlinien und -Kontrollen verstoßen könnten.
Diese Richtlinie deckt vier wichtige Phasen des Lebenszyklus von Vorfällen ab: Erkennung/Berichterstattung, Triage, Eindämmung/Behandlung und Nachbereitung des Vorfalls. Jede Phase hat klar definierte Ziele, einige wichtige Richtlinien und zugewiesene Verantwortlichkeiten.

Risikomanagement

COCUS hat einen Risikomanagementprozess implementiert, um die Identifizierung, Bewertung, Behandlung und Überwachung von Risiken zu unterstützen, die sich auf die Vertraulichkeit, Integrität, Verfügbarkeit und den Schutz personenbezogener Daten, Kundendaten und Informationssysteme auswirken könnten.

Krisenmanagement und Business Continuity

COCUS hat einen Krisenmanagementprozess für Krisensituationen eingerichtet, die sich auf das COCUS-Geschäft auswirken können. COCUS hat auch eine Business-Impact-Analyse für kritische Systeme definiert.

Ziel dieser Prozesse ist es, die organisatorische Stabilität aufrechtzuerhalten und die Wiederherstellung wesentlicher Geschäftsfunktionen im Falle einer Störung oder Krise effektiv zu koordinieren. COCUS stellt sicher, dass Disaster-Recovery-Pläne und Backup-Richtlinien regelmäßig getestet werden, um die Kontinuität von Geschäft und Betrieb zu gewährleisten.

Risikomanagement durch Dritte

COCUS bewertet neue Drittanbieter, um sicherzustellen, dass sie mit der COCUS-Sicherheit, den Datenschutzstandards und den Best Practices übereinstimmen.
Mit diesen Dritten werden formelle Vereinbarungen getroffen, die gegebenenfalls klar definierte Verantwortlichkeiten, Protokolle für das Management von Informationssicherheitsvorfällen, eingerichtete Kommunikationskanäle und benannte Ansprechpartner für Sicherheits- und Datenschutzfragen umfassen.
Darüber hinaus führt COCUS regelmäßige Due-Diligence-Prüfungen auf der Grundlage des Risikoniveaus des Drittanbieters durch, um sicherzustellen, dass seine Informationssicherheit und sein Datenschutzstatus stark bleiben und dass sein Engagement im Laufe der Zeit nicht nachgelassen hat.

Audit- und Compliance-Management

COCUS führt regelmäßige Audits durch, um die Einhaltung von Sicherheitsrichtlinien, -standards und -vorschriften zu bewerten.

Sichere Softwareentwicklung

COCUS hat Best Practices für die Sicherheit etabliert, die in den Lebenszyklus der Softwareentwicklung integriert werden sollen.

Datenschutz-Management

Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen

COCUS verpflichtet sich zur Einhaltung von Datenschutzbestimmungen und -standards, indem es Datenschutz- und Datenschutzaspekte in jede Phase seiner Verarbeitungsaktivitäten integriert – von den frühesten Phasen eines neuen Prozesses, Systems oder Produkts an. Um dies zu erreichen, müssen alle Kundenprojekte einen Sicherheitsanforderungsprozess durchlaufen, der sicherstellt, dass die Informationssicherheits- und Datenschutzteams frühzeitig einbezogen werden, um Risiken zu bewerten und geeignete Maßnahmen zur Risikominderung zu definieren.

COCUS hat eine Richtlinie zum Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen eingeführt, um sicherzustellen, dass Prozesse, Systeme und Produkte so entwickelt werden, dass die Erhebung und Verarbeitung personenbezogener Daten auf das für den angegebenen Zweck erforderliche Maß beschränkt wird.

Kundendaten

COCUS nimmt es ernst, Kundendaten zu schützen. Wir setzen uns für den Schutz der Daten unserer Kunden ein und nehmen diese Verantwortung ernst. Bei COCUS werden alle COCUS-Mitarbeiter kontinuierlich geschult und verstehen, wie sie sicher mit Kundendaten umgehen können, um ihre Privatsphäre und Vertraulichkeit zu schützen.
COCUS übernimmt und hält sich vollständig an die Anforderungen der DSGVO, was unser Engagement für die Aufrechterhaltung höchster Datenschutzstandards widerspiegelt.

Zusammenfassung

Sicherheit und Datenschutz sind bei COCUS ein fortlaufender Prozess. Wir nehmen diese Verantwortung ernst und arbeiten täglich daran, Informationen zu verbessern und zu sichern. Der Schutz von Benutzerdaten hat für alle COCUS-Infrastrukturen, Anwendungen und Betriebsaktivitäten oberste Priorität.

Um dies zu erreichen, verlässt sich COCUS auf talentierte, qualifizierte Fachleute, branchenführende Technologie zur Bewältigung von Risiken sowie klar definierte Richtlinien und Prozesse, die sicherstellen, dass alles optimal funktioniert. Mit einer Denkweise, die auf kontinuierliche Verbesserung ausgerichtet ist, bleiben wir den höchsten Standards in Bezug auf Sicherheit und Datenschutz verpflichtet.

Inhalt überprüft am 5. März 2025.