Informationssicherheitsrichtlinie (Öffentliche Version)

Inkrafttretungsdatum: Juni, 2026

Einleitung

Bei COCUS hat der Schutz von Informationen sowie die Einhaltung höchster Standards in den Bereichen Informationssicherheit, Datenschutz und Geschäftskontinuität höchste Priorität. Unser Engagement gewährleistet die Vertraulichkeit, Integrität und Verfügbarkeit aller Systeme und Daten, die für unsere Geschäftstätigkeit sowie für unsere Kunden von entscheidender Bedeutung sind. Wir verbessern kontinuierlich unser Informationssicherheits-Managementsystem (ISMS), unsere Sicherheitsmaßnahmen, Technologien sowie das Sicherheitsbewusstsein unserer Mitarbeitenden, um den fortlaufenden Schutz von Informationen und die Einhaltung aller geltenden gesetzlichen, regulatorischen und vertraglichen Anforderungen sicherzustellen. Informationssicherheit ist eine gemeinsame Verantwortung der gesamten Organisation. Das Management bekräftigt dieses Engagement durch die Einführung und Weiterentwicklung des Informationssicherheits-Managementsystems (ISMS), die Bereitstellung angemessener Ressourcen, die Kommunikation von Sicherheitszielen sowie die Förderung einer Kultur der kontinuierlichen Verbesserung. Dieses Dokument gibt einen Überblick über den Ansatz von COCUS zum Schutz von Informationen und zur Einhaltung international anerkannter Standards und bewährter Verfahren.

Organisatorische Sicherheit

Spezialisierte Sicherheitsteams

COCUS verfügt über spezialisierte Teams, die für Informationssicherheit und Datenschutz verantwortlich sind:

Information Security Team

Verantwortlich für die Steuerung der Informationssicherheit, das Risiko- und Vorfallmanagement, die Sensibilisierung der Mitarbeitenden, die Einhaltung von Vorschriften, das Informationssicherheits-Managementsystem (ISMS) sowie das Business Continuity Management.

Data Protection Team

Verantwortlich für die Einhaltung der geltenden Datenschutzgesetze und -vorschriften sowie für die Unterstützung von COCUS in seiner Rolle als Verantwortlicher und Auftragsverarbeiter im Sinne des Datenschutzes.

IT Secure Operations Team

Verantwortlich für den sicheren IT-Betrieb, einschließlich Schwachstellenmanagement, Überwachung, Identitäts- und Zugriffsmanagement, Reaktion auf Sicherheitsvorfälle, Ausfallsicherheit der IT-Infrastruktur sowie die Umsetzung von Sicherheitsmaßnahmen zur Unterstützung der Geschäftskontinuität.

Integriertes Informationssicherheits-Managementsystem

> COCUS hat ein Informationssicherheits-Managementsystem (ISMS) gemäß ISO/IEC 27001 eingeführt und betreibt dieses dauerhaft. Zudem unterstützt das ISMS die Einhaltung der Anforderungen von TISAX®. Der Geltungsbereich des ISMS umfasst:
> Die Konzeption, Entwicklung, Bereitstellung, den Betrieb und den Support einer sicheren IT-Infrastruktur sowie von Beratungsdienstleistungen, einschließlich industrieller privater Netzwerke, digitaler Produkte, Datenanalyse- und KI-/ML-Lösungen, Infrastruktur- und Netzwerkautomatisierung sowie proaktiver IT-Sicherheits- und Compliance-Dienstleistungen. Das Informationssicherheits-Managementsystem (ISMS) besteht aus Richtlinien, Standards, Verfahren und technischen Sicherheitsmaßnahmen, die darauf ausgelegt sind, Informationssicherheitsrisiken systematisch zu identifizieren, zu bewerten und zu steuern.

Diese Dokumente werden den relevanten Mitarbeitenden und Auftragnehmern kommuniziert, mindestens einmal jährlich überprüft und umfassen unter anderem folgende Themen: Informationssicherheits-Governance, Informationsklassifizierung, Risikomanagement, Identitäts- und Zugriffsmanagement, sicherer IT-Betrieb, Incident Management, Business Continuity Management, Sicherheit von Drittanbietern, Personalsicherheit, Datenschutz, sichere Softwareentwicklung sowie Asset Management. Das Informationssicherheitsteam überwacht die Einhaltung dieser Richtlinien und unterstützt deren kontinuierliche Verbesserung.

Informationsklassifizierung

COCUS hat einen Prozess zur Informationsklassifizierung eingeführt, um sicherzustellen, dass Informationen entsprechend ihrer Sensibilität und ihres geschäftlichen Werts identifiziert, verarbeitet, gespeichert, übertragen und entsorgt werden. Die Informationsklassifizierung unterstützt den Schutz der Vertraulichkeit, Integrität und Verfügbarkeit während des gesamten Lebenszyklus von Informationen.

Confidentialitätsvereinbarungen

Mitarbeitende, Auftragnehmer, Partner und Dienstleister, die Informationen von COCUS oder dessen Kunden verarbeiten, sind – sofern zutreffend – verpflichtet, Vertraulichkeits- und Geheimhaltungsvereinbarungen zu unterzeichnen, um sensible Informationen während der gesamten Dauer ihrer Tätigkeit zu schützen.

Personalsicherheit

Mitarbeitende, Auftragnehmer und andere autorisierte Nutzer, die auf Informationen oder Systeme von COCUS zugreifen, sind verpflichtet, während der gesamten Dauer ihrer Tätigkeit die geltenden Sicherheitsrichtlinien einzuhalten. Sicherheitsrelevante Verantwortlichkeiten werden vor der Vergabe von Zugriffsrechten kommuniziert und gelten auch nach Beendigung des Arbeits- oder Vertragsverhältnisses fort.

Verhaltenskodex

Der Verhaltenskodex und die internen Regelungen von COCUS legen die Verantwortlichkeiten der Mitarbeitenden hinsichtlich der ordnungsgemäßen Nutzung und des Schutzes von Unternehmensinformationen fest. Verstöße gegen Sicherheitsrichtlinien oder den Verhaltenskodex können gemäß den geltenden gesetzlichen Bestimmungen disziplinarische Maßnahmen nach sich ziehen.

Sicherheits- und Datenschutzbewusstsein

COCUS unterhält ein umfassendes Programm zur Sensibilisierung für Informationssicherheit, das unter anderem Folgendes umfasst:

- Schulungen zu Informationssicherheit und Datenschutz im Rahmen des Onboardings
- Regelmäßige Auffrischungsschulungen
- Zielgruppenspezifische, rollenbasierte Sicherheitsschulungen
- Unternehmensweite Sicherheitswarnungen und Sensibilisierungskampagnen
- Kontinuierliche Kommunikation über aktuelle Bedrohungen und bewährte Sicherheitspraktiken

Offboarding Prozesse

COCUS verfügt über formalisierte Offboarding-Prozesse, um sicherzustellen, dass:

- Zugriffsrechte unverzüglich entzogen werden
- Unternehmenseigentum zurückgegeben wird
- Informationen weiterhin geschützt bleiben
- Vertraulichkeitsverpflichtungen, soweit anwendbar, auch nach Beendigung des Arbeitsverhältnisses fortbestehen

Infrastruktursicherheit

COCUS hat Richtlinien, Standards und operative Verfahren etabliert, um seine IT-Infrastruktur, Netzwerke, Systeme und Informationswerte während ihres gesamten Lebenszyklus zu schützen.

Diese umfassen Sicherheitsmaßnahmen in den Bereichen Identitäts- und Zugriffsmanagement, Passwortmanagement, sicherer IT-Betrieb, Asset Management, sichere Konfiguration, Schwachstellenmanagement, Patch Management, Protokollierung und Überwachung, Kryptografie sowie Change Management.

Zu den technischen und organisatorischen Sicherheitsmaßnahmen gehören unter anderem Verschlüsselung, Authentifizierungsmechanismen, Endgeräteschutz, Schwachstellenmanagement, zentrale Protokollierung sowie ein sicheres Konfigurationsmanagement. Für weitere Informationen zu unserem Informationssicherheits-Managementsystem (ISMS) wenden Sie sich bitte an das Informationssicherheitsteam.

Physische Sicherheit

Der Zugang zu den Einrichtungen von COCUS ist ausschließlich autorisiertem Personal gestattet. Sicherheitszonen, physische Zutrittskontrollen, Besuchermanagement sowie Maßnahmen zum Schutz vor Umwelteinflüssen werden eingesetzt, um Einrichtungen und kritische Infrastrukturen zu schützen.

Sicherheitsbetrieb

Schwachstellenmanagement

COCUS identifiziert, bewertet, priorisiert und behebt kontinuierlich Schwachstellen, die seine Infrastruktur und Dienstleistungen betreffen, mithilfe eines strukturierten Schwachstellenmanagementprozesses.

Patch Management

Systeme werden gemäß definierten Prozessen auf Grundlage von Herstellerempfehlungen, Risikobewertungen, betrieblichen Auswirkungen und geschäftlicher Kritikalität mit Sicherheitsupdates versorgt.

Sicherheitsupdates werden regelmäßig überprüft und, sofern erforderlich, nach entsprechender Prüfung und Freigabe implementiert.

Penetrationstests

Unabhängige Penetrationstests werden in regelmäßigen Abständen nach anerkannten Industriestandards durchgeführt, um die Wirksamkeit der implementierten Sicherheitsmaßnahmen zu bewerten.

Change Management

Änderungen an Produktivumgebungen erfolgen nach einem formellen Change-Management-Prozess, der Planung, Risikobewertung, Tests, Freigabe, Implementierung sowie eine Überprüfung nach der Umsetzung umfasst.

Funktionstrennung

Verantwortlichkeiten werden angemessen voneinander getrennt, um das Risiko unbefugter oder unbeabsichtigter Aktivitäten zu reduzieren und eine angemessene Kontrolle sicherzustellen.

Asset Management

COCUS führt ein Verzeichnis seiner Informationswerte, einschließlich Hardware, Software, Cloud-Dienste und Geschäftsanwendungen.

Diese Informationswerte werden während ihres gesamten Lebenszyklus verwaltet, einschließlich Eigentümerschaft, Klassifizierung, sicherer Konfiguration, Wartung und sicherer Entsorgung.

Identitäts- und Zugriffsmanagement

Der Zugriff auf Informationen und Systeme wird entsprechend den geschäftlichen Anforderungen und dem Prinzip der geringsten Privilegien vergeben.

Zugriffsrechte werden regelmäßig überprüft und unverzüglich entzogen, sobald sie nicht mehr erforderlich sind.

Datensicherungen

Backup-Prozesse werden auf Grundlage geschäftlicher Anforderungen und der Ziele für die Notfallwiederherstellung implementiert.

Wiederherstellungstests werden regelmäßig durchgeführt, um sicherzustellen, dass Sicherungsdaten innerhalb der definierten Wiederherstellungsziele erfolgreich wiederhergestellt werden können.

Endgerätesicherheit

COCUS schützt Endgeräte durch zentral verwaltete Sicherheitsmaßnahmen, darunter Geräteverwaltung, Schutz vor Schadsoftware, Verschlüsselung, sichere Konfiguration sowie kontinuierliche Überwachung.

Sicherheitsvorfallmanagement

COCUS verfügt über formalisierte Verfahren zum Management von Sicherheitsvorfällen, die die Vertraulichkeit, Integrität, Verfügbarkeit oder den Datenschutz beeinträchtigen.

Diese Richtlinie umfasst die vier wesentlichen Phasen des Lebenszyklus eines Sicherheitsvorfalls: Erkennung und Meldung, Analyse und Priorisierung, Eindämmung und Behandlung, Wiederherstellung sowie die Nachbereitung mit Dokumentation der gewonnenen Erkenntnisse und kontinuierlicher Verbesserung.

Risikomanagement

COCUS wendet einen strukturierten Risikomanagementprozess an, um Informationssicherheitsrisiken zu identifizieren, zu bewerten, zu behandeln, zu überwachen und regelmäßig zu überprüfen.

Das Risikomanagement unterstützt fundierte Entscheidungen sowie die kontinuierliche Verbesserung der Sicherheitsmaßnahmen.

Krisenmanagement und Business Continuity Management

COCUS hat Prozesse für das Krisenmanagement und das Business Continuity Management etabliert, um die organisatorische Resilienz sicherzustellen.

Ziel dieser Prozesse ist es, die Stabilität der Organisation aufrechtzuerhalten und die Wiederherstellung wesentlicher Geschäftsprozesse im Falle einer Störung oder Krise wirksam zu koordinieren.

COCUS stellt sicher, dass Disaster-Recovery-Pläne und Backup-Richtlinien regelmäßig getestet werden, um die Kontinuität des Geschäftsbetriebs und der operativen Abläufe sicherzustellen.

Risikomanagement für Drittanbieter

COCUS bewertet Lieferanten vor der Zusammenarbeit, um sicherzustellen, dass sie angemessene Anforderungen an die Informationssicherheit und den Datenschutz erfüllen. Mit diesen Drittanbietern werden formelle Vereinbarungen geschlossen, die – sofern anwendbar – klar definierte Verantwortlichkeiten, Verfahren zum Management von Informationssicherheitsvorfällen, festgelegte Kommunikationswege sowie benannte Ansprechpartner für Informationssicherheits- und Datenschutzthemen umfassen.

Abhängig von der Kritikalität des jeweiligen Lieferanten werden regelmäßig Due-Diligence-Prüfungen durchgeführt, um die fortlaufende Einhaltung der Anforderungen sowie bestehende Risiken zu überwachen.

Audit und Compliance

COCUS führt regelmäßig interne und externe Audits durch, um die Einhaltung geltender Richtlinien, Standards, vertraglicher Verpflichtungen sowie gesetzlicher Anforderungen zu überprüfen. Die Ergebnisse dieser Audits unterstützen die kontinuierliche Verbesserung des Informationssicherheits-Managementsystems (ISMS).

Sichere Softwareentwicklung

COCUS integriert Informationssicherheit über den gesamten Softwareentwicklungszyklus hinweg, indem sichere Entwicklungspraktiken, Sicherheitstests, Maßnahmen zur Sicherstellung der Codequalität sowie ein kontrolliertes Change Management entsprechend den jeweiligen Risiken angewendet werden. Data Protection Management

Datenschutz durch Technikgestaltung und datenschutzfreundliche Voreinstellungen

Datenschutz- und Informationssicherheitsanforderungen werden bereits in den frühesten Phasen von Projekten, Systemen und Dienstleistungen berücksichtigt.

Alle Kundenprojekte durchlaufen einen Sicherheitsbewertungsprozess unter Beteiligung der Teams für Informationssicherheit und Datenschutz, um Risiken zu identifizieren und geeignete Maßnahmen zur Risikominderung festzulegen.

COCUS wendet die Grundsätze des Datenschutzes durch Technikgestaltung und datenschutzfreundliche Voreinstellungen an, um sicherzustellen, dass die Verarbeitung personenbezogener Daten auf das für den vorgesehenen Zweck erforderliche Maß beschränkt bleibt.

Informationsschutz

COCUS schützt sensible Informationen durch eine Kombination aus technischen und organisatorischen Maßnahmen, darunter Informationsklassifizierung, rollenbasierte Zugriffskontrollen, Verschlüsselung, sichere Kollaborationsplattformen, Informationsschutzfunktionen von Microsoft 365, sichere Konfiguration von Unternehmenssystemen sowie die Überwachung und Protokollierung von Zugriffen auf sensible Informationen.

Diese Maßnahmen tragen dazu bei, das Risiko einer unbefugten Offenlegung, Veränderung oder eines Verlusts von Informationen zu reduzieren.

Kundendaten

Der Schutz von Kundendaten hat für COCUS höchste Priorität. Wir verpflichten uns umfassend zum Schutz der Daten unserer Kunden und nehmen diese Verantwortung sehr ernst.

Mitarbeitende werden regelmäßig im sicheren Umgang mit Kundeninformationen geschult. Darüber hinaus werden geeignete technische und organisatorische Maßnahmen umgesetzt, um die Vertraulichkeit, Integrität und Verfügbarkeit der Informationen während ihres gesamten Lebenszyklus zu gewährleisten. COCUS erfüllt die Anforderungen der Datenschutz-Grundverordnung (DSGVO) sowie weiterer anwendbarer Datenschutzvorschriften.

1.1 Kontinuierliche Verbesserung

Informationssicherheit ist bei COCUS ein fortlaufender Prozess und eine dauerhafte Verpflichtung.

Wir überprüfen und verbessern kontinuierlich unser Informationssicherheits-Managementsystem (ISMS), unsere Prozesse, Technologien sowie unsere Sensibilisierungsprogramme, um auf sich verändernde

Bedrohungen, neue geschäftliche Anforderungen und regulatorische Vorgaben angemessen reagieren zu können.

Durch qualifizierte Fachkräfte, eine wirksame Governance, sichere Technologien und eine gelebte Sicherheitskultur verpflichtet sich COCUS, Informationen zu schützen und das Vertrauen seiner Kunden, Partner und Mitarbeitenden dauerhaft zu erhalten.