OPITZ CONSULTING

Informationssicherheitsrichtlinie (extern)

ISO 27001

Verantwortlicher	ISO	Informationsklassifikation	öffentlich
Autore(n)	FHU, FKR	Geltungsbereich	OCD
Dokumententyp	Richtlinie	Gültigkeit ab	11.03.2022
Version	2.0	Letzte Aktualisierung	16.03.2023 10:36:00
DocID (Sharepoint)	DOCIDPRJ-1134-405	Freigabe (optional)	08.10.2021 TSC

Inhalt

1. Einleitung und Geltungsbereich

Informationen gehören zu den wichtigsten Gütern von IT-Unternehmen. Informationen über Patente, Design, Finanzen, Prozesse, Kunden, Zulieferer, Partner und Mitarbeiter sind elementar für den Unternehmenserfolg. Der Schutz und die Absicherung dieser Informationen sind daher sowohl für das Kerngeschäft wichtig, als auch in vielen Fällen gesetzlich vorgeschrieben und darüber hinaus ein fundamentaler Bestandteil der Corporate Governance (Leitlinie) der OPITZ CONSULTING Deutschland GmbH.

Diese Richtlinie bildet die Basis für das Rahmenwerk an Anforderungen der Informationssicherheit für OPITZ CONSULTING Deutschland GmbH.

Es liegt in der Verantwortung der angesprochenen Zielgruppen, die Informationssicherheitsinitiativen zu unterstützen und den Anforderungen der Informationssicherheit zu entsprechen.

Die vorliegende Richtlinie ist für den öffentlichen Gebrauch. Alle weiteren Richtlinien sind grundsätzlich nur unternehmensintern zu halten. Bei Bedarf wird der ISO darüber befinden, ob sie an Dritte (z. B. Kunden, Vertragspartner, Lieferanten) weitergegeben werden können.

2. Grundlegende Begriffe und Abkürzungen (Glossar)

Begriff	Erläuterung
Authentizität	Echtheit von Informationen oder Identitäten durch ■ Authentifizierung: Prüfung und Nachweis der Identität (oder anderer Eigenschaften) einer Person oder Entität ■ Authentisierung: Vorgang des Nachweises der eigenen Identität (oder anderer Eigenschaften) durch eine Person oder Entität
Informationssicherheit	Gewährleistung und Erhalt der Vertraulichkeit, Integrität und Verfügbarkeit von Informationen; weitere Attribute wie Authentizität, Verantwortlichkeit, Verbindlichkeit und Zuverlässigkeit können auch betrachtet werden.
Informationssicherheits-Managementsystem (ISMS)	Grundsätze, Planungsaktivitäten, Verantwortung, Prozesse, Verfahren und Ressourcen zur Sicherstellung der Informationssicherheit
Informations-verfügbarkeit	Gewährleistung des bedarfsorientierten Zugriffs auf Informationen und zugehörigen Werten für berechtigte Benutzer
Integrität	Sicherstellung von Vollständigkeit und Richtigkeit der Informationen und ihrer Verarbeitungsmethoden

Begriff	Erläuterung
ISO	Informationssicherheitsbeauftragter (Information security officer)
ISSC	Steuerkreis Informationssicherheit (Information security steering circle)
Richtlinie (Policy)	Allgemeine Anweisung, die formell durch das Management ausgesprochen wird.
Verbindlichkeit (nicht Abstreitbarkeit)	Niemand kann das Senden oder Empfangen von Informationen abstreiten/ leugnen: ■ Proof of origin: Empfänger kann Ursprung der Informationen nachweisen ■ Proof of delivery: Sender kann Auslieferung von Informationen beweisen
Verlässlichkeit	Sicherstellung eines konsistenten Verhaltens und Lieferung vorgesehener (intendierter) Ergebnisse durch eine Person oder Entität
Vertraulichkeit	Gewährleistung des Zugriffs auf Informationen nur für die Zugangsberechtigten
Wert/Asset	Jede Art von (Vermögens-) Wert eines Unternehmens oder einer Organisation, wie z. B. ■ Informationen ■ Software, ■ Computerprogramme ■ Physische Vermögenswerte wie Rechner ■ Dienste (Services) ■ Menschen und ihre Qualifikationen, Fähigkeiten, Erfahrungen ■ Immaterielle Werte wie Reputation und Ansehen
Zurechenbarkeit (Verantwortlichkeit)	Übernahme von Verantwortung, Rechenschaft und/oder Haftung für Informationswerte (Assets) (Zugriffskontrolle, Korrektheit/Sicherheit der Informationen)

3. Ziele und grundlegende Prinzipien der Informationssicherheit

Das OC Informationssicherheitsmanagement verringert Risiken durch die Analyse von Sicherheitsbedrohungen und der Einleitung entsprechender Schutzmaßnahmen mit Hilfe der Implementierung von technischen, organisatorischen und personellen Regelungen, die durch das identifizierte Risiko gerechtfertigt sind.

Informationssicherheitsregelungen, -prozesse und -methoden müssen in Einklang mit denen des Unternehmensdatenschutzes, des Unternehmensrisikomanagements und der Unternehmenssicherheit stehen.

Die OC Informationssicherheitsanforderungen sind in Anlehnung an die ISO 27000 Reihe im OC Informationsmanagementsicherheitssystem definiert (z. B.: Einstufung und Handhabung von Informationen, Anforderungen an Passwörter, technische Aspekte).

Das Kernziel der Informationssicherheit ist es die folgenden fünf Ziele sicherzustellen:

- Vertraulichkeit - Sicherstellung, dass nur Personen Zugriff auf Informationen haben, die sie im Rahmen ihrer Tätigkeit auch benötigen ("need to know")
- Integrität - Sicherstellung der Richtigkeit und Vollständigkeit von Informationen und Verarbeitungsmethoden
- Verfügbarkeit - Sicherstellung, dass autorisierte Benutzer jederzeit Zugriff auf benötigte Informationen, Rechenzentren und Dienste haben
- Verlässlichkeit - Sicherstellung, dass auf Informationen vertraut werden kann, d.h. Informationen sind echt, verifizierbar und die Kommunikationswege sind nachvollziehbar
- Verantwortlichkeit/Verbindlichkeit -Sicherstellung, dass alle Nutzer (Mitarbeiter, Partner, Kunden und Prozesse) für ihr Handeln zur Verantwortung gezogen werden können

OC-Informationssicherheitsprozesse müssen unter Einhaltung der Prinzipien dieser Richtlinie sowie dem Informationssicherheitsmanagementsystem (ISMS) entworfen und organisiert werden. Dies stellt die effiziente Umsetzung sowie die unternehmensweite Konsistenz sicher.

Alle Informationssicherheitsmaßnahmen, sowohl organisatorisch als auch technisch, stehen in einem wirtschaftlich vertretbaren Verhältnis zum Wert der schützenswerten Informationen und IT-Systeme. Darüber hinaus ist zu gewährleisten das die getroffenen sicherheitstechnischen Maßnahmen praxisgerecht und transparent für den Benutzer sind.

Negative finanzielle und immaterielle Folgen für das Unternehmen sowie für die Mitarbeiter durch Gesetzesverstöße sind zu vermeiden. Alle Mitarbeiter der OPITZ CONSULTING Deutschland GmbH sind auf die Einhaltung der einschlägigen Gesetze, wie z.B. dem Strafgesetzbuch, oder dem Bundesdatenschutzgesetz, und die sich aus dem Vertrag des Mitarbeiters ergebenden Bindungen verpflichtet.

Die Geschäftsführung und die Mitarbeiter der OPITZ CONSULTING Deutschland GmbH sind sich ihrer Verantwortung beim Umgang mit Informationsverarbeitungssystemen bewusst und unterstützen das Informationssicherheitsmanagement. Die OPITZ CONSULTING Deutschland

GmbH stellt entsprechende Mittel zur Verfügung, um die Mitarbeiter bei ihren Tätigkeiten diesbezüglich im angemessenen Rahmen unterstützen.

4. Rollen und Verantwortlichkeiten des Managementkreises

Informationssicherheit betrifft jeden OC-Mitarbeiter (inkl. GF und Managementkreis) und muss auf jeden Vertragspartner und Lieferant ausgeweitet werden. Jeder OC-Mitarbeiter und Vertragspartner sowie Lieferant ist verantwortlich für die Unternehmensinformationen, die er handhabt.

4.1. OC-Mitarbeiter, GF und Mitglieder des Managementkreises

Die GF wird die Sicherheitsorganisation und den Sicherheitsprozess aktiv unterstützen und notwendige Ressourcen bereitstellen. Die GF wird sich an dem Standard ISO/IEC 27001 orientieren und die Management-Elemente dieses Standards realisieren. Diese umfassen die Durchführung von regelmäßigen internen Audits, eine geeignete Dokumentenlenkung, die Managementbewertung und die Anwendung des Modells der kontinuierlichen Verbesserung (PDCA).

Jedes Mitglied des Managementkreises hat darüber hinaus die Aufgabe, die Informationssicherheit in seinem Bereich sicherzustellen.

Jeder Mitarbeiter spielt eine wichtige Rolle bei der Wahrung der Informationssicherheit innerhalb seines Verantwortungsbereichs. Dies wird durch die Einhaltung, der im ISMS vorgeschriebenen Anforderungen der Informationssicherheit sichergestellt. Jeder Mitarbeiter ist verpflichtet, die allgemeinen sowie die für den jeweiligen Arbeitsplatz geltenden (Sicherheits-) Richtlinien und Vorgaben zu beachten und einzuhalten sowie Sicherheitsvorkommnisse umgehend zu melden.

4.2. Vertragspartner bzw. Lieferant

Auch externe Vertragspartner und Lieferanten verpflichten sich auf diese Leitlinie. Für relevante Lieferanten, wozu z. B. Unterauftragnehmer für IT-Dienstleistungen gegenüber OC Kunden zählen, gelten weiterführende einzuhaltende Sicherheitsanforderungen, welche in der „IT-Sicherheitsrichtlinie für Auftragnehmer“ dokumentiert sind.

4.3. Steuerkreis Informationssicherheit (ISSC)

Der Steuerkreis steht unter dem Vorsitz des Head of Controlling & Administration der OPITZ CONSULTING Deutschland GmbH und handelt mit der vollen Ermächtigung der gesamten Geschäftsleitung. Mitglieder sind der IT-Leiter, der Informationssicherheitsbeauftragte, der Datenschutz-beauftragte und ggf. Anwendervertreter.

Die Verantwortlichkeiten des ISSC sind:

- Definition und Überprüfung des OC Informationssicherheits-managementsystems
- Definition von Anforderungen der Informationssicherheit zur Verringerung von Sicherheitsrisiken
- Zuweisung von Aufgaben mit Bezug auf Informationssicherheit
- Überwachen des Status der Informationssicherheit im Rahmen von regelmäßigen Sicherheitsreviews (Teilnehmer: ISO, DSB, IT-Leiter und Anwendervertreter), Bericht an die Geschäftsführung
- Kontinuierliche Verbesserung der Informationssicherheit in den einzelnen Geschäftsbereichen und Niederlassungen
- Steuerung von Katastrophenfällen
- Durchführung eines regelmäßigen Managementreviews

4.4. Informationssicherheitsbeauftragter (ISO)

In Zusammenarbeit mit dem ISSC ist der ISO für die Umsetzung und Verbesserung der Informationssicherheit innerhalb von OC zuständig.

Die Verantwortlichkeiten des ISOs sind:

- Aufbau und Weiterentwicklung des zentralen ISMS
- Verbesserung der Informationssicherheit auf strukturierte und systematische Weise in Zusammenarbeit mit anderen Sicherheitsfunktionen und entsprechend den Geschäftsrisiken
- kontinuierliche Durchführung von Sicherheitsprüfungen, -tests und -stichproben, um eine Prüfung der Wirksamkeit laufender Maßnahmen und Prozesse gemäß den Vorgaben des ISSC zu ermöglichen
- Erhöhung des Sicherheitsbewusstseins der Mitarbeiter
- Betrieb eines Berichtswesens
- Firmenweiter Ansprechpartner hinsichtlich der sicheren Handhabung von Informationen
- Vorbereitung des Managementreviews
- Planung und Durchführung von Lieferantenaudits

4.5. Interner ISMS Auditor

Die Verantwortlichkeiten des internen ISMS Auditors sind:

- Durchführung von Kontrollen der Wirksamkeit und internen Audits zur Einhaltung des ISMS
- Erarbeitung von Verbesserungsvorschlägen
- Report an den IT-Sicherheitsbeauftragten (Vorbereitung Managementreview)

4.6. Datenschutzbeauftragter

Die Verantwortlichkeiten des Datenschutzbeauftragten sind:

- Überwachung der Einhaltung der relevanten Datenschutzvorschriften
- Sicherstellung der Konsistenz der Richtlinien auf dem Gebiet des Datenschutzes
- Durchführung von Datenschutzkontrollen entsprechend den gesetzlichen Anforderungen

Technische und organisatorische Maßnahmen des Datenschutzes müssen gesetzliche Vorgaben einhalten.

5. Konformität und Prüfung

Die Prüfung der Einhaltung von Anforderungen der Informationssicherheit erfolgt durch:

- Interne Kontrollen der Standorte im Geltungsbereich
- Laufende Überprüfungs- und Bewertungsprozesse des ISO und des internen Auditors
- Managementreview

Diese Ergebnisse werden dazu verwendet, Schwerpunkte und Verbesserungspotentiale der Informationssicherheit unternehmensweit zu identifizieren.

Die Prozesse der Informationssicherheit müssen den rechtlichen Vorgaben in Deutschland entsprechen.

Relevante Vorgaben ergeben sich aus den folgenden Gesetzen:

- Bundesdatenschutzgesetz und EU-Datenschutzgrundverordnung
- IT-Sicherheitsgesetz 2.0
- Arbeitsschutzgesetze
- Sozialgesetzbücher
- BGB und HGB
- Geschäftsgeheimnisgesetz
- Gesetz gegen den unlauteren Wettbewerb

6. Versionshistorie

Version	Durch Wen	Veränderung
V 1.0	JOH	Initiale Erstellung
V 2.0	JOH / FHU	CI-Umstellung
V 2.1	FKR/FHU	■ 5.1 Anpassungen Managementverantwortlichkeiten, ■ 5.3 Präzisierung der Aufgaben des ISSC und Abgrenzung Managementreview ■ 6. Aufnahme Geschäftsgeheimnisgesetz
V 2.2	FKR/FHU	■ Anpassungen Metadatenstruktur und Dokumentensteuerungsstruktur ■ Aufnahme neues IT-Sicherheitsgesetz 2.0 und Gesetz gegen den unlauteren Wettbewerb ■ 4.2: Aufnahme der „IT-Sicherheitsrichtlinie für Auftragnehmer“ ■ 4.3: Aufnahme des IT-Leiters in den Steuerkreis Informationssicherheit (ISSC) ■ 5: Aufnahme des internen Auditors in die Prüfzyklen
V 2.3	FKR/FHU	■ Änderung des Namens in Informationssicherheitsrichtlinie (extern) ■ Überprüfung des Dokumentes
V 2.3	FHU/FKR	23.02.2023 ■ Überprüfung auf Aktualität – keine Änderung erforderlich

Tab. 1. Versionshistorie