Konzernrichtlinie 7

Globale Informations- und Systemsicherheit

Zweck

Das Ziel dieser Richtlinie besteht darin, die Verpflichtung von Stryker zu angemessenen Sicherheitskontrollen für seine Informationen, Systeme und Operationen zu erläutern, die im Einklang mit dem geltenden Recht stehen.

Geltungsbereich

Diese Richtlinie gilt für alle Stryker-Mitarbeiter und Drittparteien (z. B. Anbieter, Auftragnehmer, Beauftragte), die im Auftrag von Stryker agieren, unabhängig von ihrem Standort. Wenn eine Bestimmung in dieser Richtlinie im Widerspruch zum lokalen oder regionalen Recht steht, das für eine bestimmte Rechtseinheit von Stryker gilt, dann soll diese Einheit diese Richtlinie durch einen Anhang im notwendigen Umfang ergänzen, um das lokale oder regionale Recht einzuhalten, vorausgesetzt, dass die überarbeitete Richtlinie weitestgehend mit den in dieser Richtlinie enthaltenen Prinzipien im Einklang steht. Ein solcher Anhang muss durch den leitenden Beauftragten für Informationssicherheit (Chief Information Security Officer, CISO) genehmigt werden. Wo kein lokaler oder regionaler Anhang implementiert wurde, bleiben alle Bestimmungen dieser Richtlinie in Kraft, soweit sie im Einklang mit dem geltenden Recht stehen.

Grundsätze

Stryker wird alle Gesetze einhalten, die die Sicherheit der Produkte und Systeme von Stryker regeln. Darüber hinaus verpflichtet sich Stryker zur Einhaltung der nachfolgend aufgeführten Standards.

1. **Benennung eines leitenden Beauftragten für Informationssicherheit (Chief Information Security Officer, CISO):** Der CISO ist für die Festlegung und Durchsetzung des effektiven Betriebs des globalen Informationssicherheitsprogramms von Stryker und die Abstimmung von Sicherheitsinitiativen mit Unternehmensprogrammen und Geschäftszielen zum Schutz von Informationswerten, Produkten, Systemen und Technologien verantwortlich.

2. **Implementierung von Sicherheitsrichtlinien und administrativen und Leitungsstrukturen:** Stryker wird durch die einschlägigen Qualitätsmanagementsysteme, das Informationssicherheits-Managementsystem, die Standards für zulässige Nutzung, den Vorfallreaktionsplan und dazugehörige Standards und Verfahren angemessene administrative, technische und physische Sicherheitskontrollen implementieren.

3. **Bewertung von Drittparteien:** Der Bewertungsprozess zur globalen Sicherheit muss durchgeführt werden, bevor eine Drittpartei beauftragt wird, die Zugriff auf die Netzwerke von Stryker oder die elektronischen sensiblen Daten hat oder internetbasierte Lösungen oder Software zur internen Nutzung oder zur Nutzung in einem Stryker-Produkt oder Dienstleistungsangebot bereitstellt.

4. **Nutzung von Stryker-Geräten und -Systemen:** Jeder Stryker-Mitarbeiter oder jede Drittpartei mit Zugriff auf die Geräte oder Systeme von Stryker wird diese Geräte und Systeme im Einklang mit den geltenden Anforderungen bezüglich einer zulässigen Nutzung verwenden.

Verantwortlichkeiten

Alle Stryker-Mitarbeiter und Drittparteien sind verantwortlich, diese Richtlinie und alle geltenden Standards und Verfahren zur Implementierung einzuhalten. Der CISO muss in Zusammenarbeit mit anderen zuständigen Funktionsbereichen und Geschäftseinheiten alle zusätzlichen Standards und Verfahren festlegen, die zur Einhaltung dieser Richtlinie erforderlich sind, und derartige Standards und Verfahren vorbereiten und implementieren.

Konformität

Stryker verlangt von allen Mitarbeitern und Drittparteien die Einhaltung dieser Richtlinie. Wenn Sie eine Frage zu dieser Richtlinie oder zu den zugehörigen Verfahren, oder Bedenken hinsichtlich des Sicherheitsprogramms von Stryker haben, wenden Sie sich bitte an den lokalen Vertreter der Personalabteilung von Stryker, einen Compliance Officer, Rechtsberater oder die Ethikhotline. Stryker wird alle Berichte dieser Art im Einklang mit den Hotline-Richtlinien und -verfahren vertraulich behandeln.