Leitlinie zu Informationssicherheitsanforderungen für Vertragspartner der Vincenz Wiederholt GmbH

Fassung: Stand Juli 2024

1. Ziel und Zweck

Dieses Dokument legt die Erwartungen der Vincenz Wiederholt GmbH zum Schutz der Vertraulichkeit, Integrität und Verfügbarkeit ihrer Daten und Vermögenswerte fest.

2. Geltungsbereich

Diese Handlungsleitlinie gilt für Vertragspartner, die auf Basis vertraglicher Regelungen Lieferungen und Leistungen für die Vincenz Wiederholt GmbH erbringen.

3. IT-Sicherheits-Policy und Standards

Vertragspartner mit Zugang zu Informationen der Vincenz Wiederholt GmbH müssen deren Informationssicherheitsrichtlinien und die damit verbundenen Dokumente einhalten. Ferner müssen Vertragspartner über geeignete Cyber-Risiko-Governance-Prozesse verfügen, um das Risiko für die ihrerseits eingesetzten IT-Systeme in Bezug auf die Anforderungen an Vertraulichkeit, Verfügbarkeit und Integrität der Vincenz Wiederholt GmbH zu gewährleisten.

4. Informationssicherheitsinformation für Vertragspartner

Im Rahmen bestehender Vertrags- und Lieferbeziehungen ist es von größter Bedeutung, dass Vertragspartner den Sicherheitsinteressen und Anforderungen an die Informationssicherheit der Vincenz Wiederholt GmbH sowie deren Kunden entsprechen. Deshalb sind sämtliche mit entsprechender Klassifizierung eingestufte Umfänge (wie z. B. Design- und Entwicklungsdaten sowie andere entsprechend kritische Informationen) in geeigneter Weise zu verarbeiten und zu schützen. Im Sinne der Informationssicherheits-anforderungen der Vincenz Wiederholt GmbH hat der Vertragspartner die Verpflichtung, sämtliche Lieferungen und Leistungen, sowie den gesamten im Zusammenhang stehenden Datenbestand der Vincenz Wiederholt GmbH, nach dem Stand der Technik gegen unberechtigten Zugriff, Veränderung, Zerstörung und sonstigen Missbrauch zu sichern. Ferner sind Daten der Vincenz Wiederholt GmbH strikt von Daten anderer Kunden des Vertrags-partners zu trennen. Ist ein identifizierter, signifikanter Fall der Verletzung der Informationssicherheit eingetreten, ist der Informationssicherheitsbe-auftragte der Vincenz Wiederholt GmbH unverzüglich zu informieren.

Kontaktdaten:
Herr Kai Orlowski
Security Assist GmbH
kai.orlowski@security-assist.com
Telefon: +49 231 / 47 64 48 - 40

5. Asset Management

Der Vertragspartner hat von der Vincenz Wiederholt GmbH zur Verfügung gestellte Informationen gemäß der von Vincenz Wiederholt GmbH ange-gebenen Klassifizierung, jedoch mindestens als vertrauliche Information, zu behandeln. Für die Übertragung von Informationen ist eine starke Verschlüsselung zu verwenden. Die Weitergabe sowie Vervielfältigung von vertraulichen Unterlagen sowie die Verwertung und Mitteilung ihres Inhalts ist nicht ohne die vorherige schriftliche Genehmigung der Vincenz Wiederholt GmbH gestattet. Informationen der Vincenz Wiederholt GmbH dürfen außerhalb des vertraglich vereinbarten Verwendungszwecks nicht gespeichert, gedruckt, kopiert, weitergegeben oder auf andere Weise verarbeitet werden.

6. Benutzer-Authentifizierung

Der Zugang zu IT-Systemen des Vertragspartners bzw. auf dort befind-liche Daten der Vincenz Wiederholt GmbH, soll nur sicher identifizierten (authentifizierten) Benutzern möglich sein. Dafür muss die Identität eines Benutzers durch geeignete Verfahren sicher festgestellt sein. Es müssen Zugriffskontrollen für Informationssysteme, Netzwerke und Anwendungen implementiert sein, die

- die Identität aller Benutzer prüfen und
- den Zugriff ausschließlich auf autorisierte Benutzer beschränken.

7. Verschlüsselung von Laptops und mobilen Speichermedien

Geräte des Vertragspartners, auf denen sich Daten der Vincenz Wiederholt GmbH befinden, sind angemessen zu verschlüsseln und die Implementierung der Verschlüsselung muss kontinuierlich validiert werden. Zum Schutz von vertraulichen Informationen sind während der Übertragung über offene öffentliche Netze starke Kryptographie und Sicherheitsprotokolle (z. B. TLS, IPSEC, SSH usw.) zu verwenden.

8. Client-Systeme

Der Einsatz von EDR/XDR- sowie Anti-Spyware-Werkzeugen auf Client-Systemen des Vertragspartners wird vorausgesetzt. Alle Client-Systeme, die auf vertrauliche Daten zugreifen, müssen unabhängig davon, ob sie verwendet werden oder nicht, physisch gesichert werden. Empfangene Daten und Programme werden vor ihrer Ausführung automatisch auf Schadsoftware untersucht. Ferner wird der gesamte Dateninhalt aller Systeme regelmäßig auf Schadsoftware untersucht. Die Datenübertragung durch zentrale Gateways (z.B. E-Mail, Internet, Drittnetze) wird mit einer Schutzsoftware überprüft (einschließlich verschlüsselter Verbindungen). Client-Systeme, die von gesicherten Orten aus auf vertrauliche Daten zu-greifen, müssen über ein Passwort verfügen. Es wird ein geschützter Bild-schirmschoner gefordert bzw. muss nach spätestens 10 Minuten Inaktivität der Kontozugang gesperrt werden. Es werden Maßnahmen festgelegt, die verhindern, dass Schutzsoftware durch Benutzer deaktiviert oder verändert werden kann.

9. Mobile Geräte

Um auf Mobilgeräten gespeicherte vertrauliche Informationen zu schützen, muss der Vertragspartner eine starke Verschlüsselung verwenden.

Personenbezogene Daten dürfen nur auf Mobilgeräten mit starker Verschlüsselung gespeichert werden. Entsprechend dokumentierte Richtlinien, Verfahren und Standards müssen etabliert sein.

10. Schutz vor Schadcode

Der Vertragspartner muss über Erkennungs- und Präventionsmaßnahmen verfügen, die vor bösartiger Software schützen. Durch Schulungen zur Sensibilisierung der Benutzer ist die entsprechende Awareness zu schaffen. Der ein- und ausgehende Netzwerkverkehr ist zur Erkennung und zum Schutz von bösartigem Code entsprechend in Echtzeit zu scannen und zu filtern (E-Mail, HTTP, FTP u. andere Messaging Protokolle). Es muss verhindert werden, dass nicht autorisierter mobiler Code ausgeführt wird.

11. Physischer Anschluss von IT-Equipment

Der physische Anschluss von IT-Equipment eines Fremdunternehmens an das Netz oder an IT-Systeme der Vincenz Wiederholt GmbH ist aufgrund eines möglichen Virenbefalls oder des Risikos von Cyberangriffen grundsätzlich untersagt. Ausgenommen sind Datenträger, die durch die IT-Abteilung für eine externe Datenspeicherung zur Verfügung gestellt wurden oder durch die Geschäftsleitung genehmigt wurden. Beispiele für IT-Equipment sind: Externe Festplatten, USB-Datenträger, Notebooks, Speicherkarten, usw. Der Vertragspartner garantiert, dass sämtliche Hardware, die dann – nach erfolgter Genehmigung durch die Vincenz Wiederholt GmbH – an das Firmennetzwerk angeschlossen wird, frei von Schadsoftware ist. Hierzu hat er eine gründliche Überprüfung dieser Hardware auf Schadsoftware durchgeführt, um sicherzustellen, dass sie frei von Viren, Spyware, Ransomware oder anderen schädlichen Programmen ist. Die Hardware sollte mit den neuesten Sicherheitsupdates und Patches versehen sein, um bekannte Schwachstellen zu beheben. Dies gilt sowohl für das Betriebssystem als auch für alle installierten Anwendungen.

12. In-Kraft-Treten

Diese Leitlinie tritt am 01.08.2024 in Kraft.

Holzwickede, Datum 08.07.2024

gez. Geschäftsführung

gez. ISB