Richtlinie zur Meldung von Sicherheitslücken

1. Zweck

Zweck dieser Richtlinie zur Meldung von Sicherheitslücken ist die Bereitstellung eines klaren und sicheren Prozesses zur Offenlegung potenzieller Sicherheitslücken in unseren Produkten. Wir schätzen die Beiträge von Cybersecurity-Experten, Kunden und Partnern, die uns dabei unterstützen, die Sicherheit, Integrität und Verfügbarkeit unserer Produkte zu gewährleisten.

2. Geltungsbereich

Diese Richtlinie gilt für alle softwaregestützten In-vitro-Diagnostika-Produkte (IVD), sofern nicht ausdrücklich etwas anderes angegeben ist

3. Meldung einer Sicherheitslücke

Wenn Sie glauben, eine Sicherheitslücke identifiziert zu haben, melden Sie diese bitte über: https://app.whistle.law/whistle/ - /5a474110-2abf-4d2d-8b37-92c1c9050789

Bitte übermitteln Sie uns keine sensiblen Informationen (z. B. Patientendaten) in den bereitgestellten Dokumenten.

Bitte fügen Sie nach Möglichkeit folgende Informationen bei:

- Betroffenes Gerät: Hersteller, Modell, Hardwareversion, Firmware-/Softwareversion
- Beschreibung der Schwachstelle: Was genau haben Sie beobachtet und welche Sicherheitsauswirkungen vermuten Sie?
- Schritte zur Reproduktion: Eine möglichst detaillierte Schritt-für-Schritt-Beschreibung einschließlich Voraussetzungen, benötigter Werkzeuge und Netzwerkumgebung.
- Nachweise: Screenshots, Protokolle, Paketmitschnitte, Beispielanfragen oder andere unterstützende Dokumente. Bitte anonymisieren Sie personenbezogene Daten oder Daten Dritter.
- Potenzielle Auswirkungen: Welche Daten, Funktionen oder Systeme könnten betroffen sein? Ist physischer Zugriff, lokaler Netzwerkzugriff oder Internetzugriff erforderlich?
- Testumgebung: Haben Sie ausschließlich auf Ihren eigenen oder autorisierten Geräten getestet? Wurden Daten Dritter eingesehen, verändert oder übertragen?
- Offenlegungsstatus: Wurde die Schwachstelle bereits öffentlich bekannt gemacht oder anderen Parteien gemeldet? Ist eine öffentliche Offenlegung geplant?
- Erforderliche Kontaktdaten (Ansprechpartner, Organisationsname, Referenznummern, E-Mail-Adressen, Telefonnummern), damit wir mit Ihnen Kontakt aufnehmen können.

4. Unsere Verpflichtung

Wir verpflichten uns:

- Den Eingang Ihrer Meldung innerhalb von **5 Werktagen** zu bestätigen (Voraussetzung: Kontaktdaten wurden angegeben).
- Die Schwachstelle zeitnah zu bewerten.
- Sie, sofern angemessen, über den Status Ihrer Meldung zu informieren (Voraussetzung: Kontaktdaten wurden angegeben).
- Ihre Meldung vertraulich zu behandeln.
- Keine rechtlichen Schritte gegen Cybersecurity-Experten einzuleiten, die in guter Absicht und im Einklang mit dieser Richtlinie handeln.

5. Erwartungen an eine verantwortungsvolle Offenlegung

Wir bitten Sie:

- Handeln Sie in guter Absicht und vermeiden Sie die Verletzungen der Privatsphäre, Datenzerstörung oder Dienstunterbrechungen.
- Die Schwachstelle nicht über das zur Demonstration erforderliche Maß hinaus auszunutzen.
- Die Schwachstelle nicht öffentlich bekannt zu machen, bevor wir die Gelegenheit hatten, diese zu untersuchen und zu beheben.
- Uns ausreichend Zeit zur Behebung des Problems vor einer Veröffentlichung einzuräumen.

6. Bewertung und Bearbeitung

Gemeldete Schwachstellen werden:

- Hinsichtlich Schweregrad, Ausnutzbarkeit und möglicher Auswirkungen auf Patientensicherheit, Datenintegrität und Systemverfügbarkeit bewertet.
- Gemäß den geltenden Normen in unsere Cybersecurity- und Risikomanagementprozesse integriert.

Schwachstellen mit potenziellen Auswirkungen auf die Produktsicherheit werden im Rahmen des Risikomanagements gemäß **ISO 14971** bewertet.

7. Behebung

Falls erforderlich, werden wir:

- Geeignete Korrekturmaßnahmen entwickeln und umsetzen (z. B. Patches oder andere Gegenmaßnahmen).
- Die Wirksamkeit der umgesetzten Maßnahmen validieren.
- Relevante Informationen an betroffene Kunden kommunizieren

8. Offenlegung

Eine öffentliche Bekanntmachung (z. B. Sicherheitsmeldungen im Feld, Security Advisories oder CVE-Veröffentlichungen) wird nach Möglichkeit mit der meldenden Partei abgestimmt und erst nach Durchführung geeigneter Abhilfemaßnahmen vorgenommen.

9. Integration in Post-Market-Aktivitäten

Alle gemeldeten Schwachstellen werden als Eingaben für unsere Post-Market-Surveillance- und Cybersecurity-Risikomanagementprozesse berücksichtigt.

10. Rechtliche Hinweise

Diese Richtlinie erteilt keine Erlaubnis, auf Daten zuzugreifen oder diese zu verändern, die über das für eine verantwortungsvolle Schwachstellenforschung notwendige Maß hinausgehen. Alle Aktivitäten müssen den geltenden Gesetzen und Vorschriften entsprechen.

11. Kontakt

Bei Fragen zu dieser Richtlinie kontaktieren Sie bitte:
info@analyticon-diagnostics.com

Unterzeichnet im Namen der **Analyticon Biotechnologies GmbH**
Am Mühlenberg 10
35104 Lichtenfels, Deutschland

Dr. Stephan Busche
Geschäftsführer
Ort: Lichtenfels, Deutschland
Datum: 10.08.2026