RICHTLINIE

Koordinierte Offenlegung von Schwachstellen

Coordinated Vulnerability Disclosure (CVD) Policy der UNITEC Informationssysteme GmbH

Dokumenten-ID	UNITEC-CVD-001
Herausgeber	UNITEC Informationssysteme GmbH, Maria-Montessori-Allee 10, 63457 Hanau
Eigentümer / Pflege	CRA & Security Team – UNITEC
Version / Stand	1.0 / 09.09.2026
Freigabe	Leitung CRA & Security Team
Klassifizierung	Vertraulich – zur Weitergabe an Geschäftspartner im Rahmen der CRA-Lieferantenauskunft freigegeben
Geltungsbereich	Alle Softwareprodukte der UNITEC Informationssysteme GmbH

Geltungsbereich

Diese Regelung gilt für alle Softwareprodukte der UNITEC Informationssysteme GmbH. Sie ist produktneutral formuliert und bedarf bei neuen Produkten keiner Anpassung.

1. Unser Versprechen

Die Sicherheit unserer Softwareprodukte hat für die UNITEC Informationssysteme GmbH hohe Priorität. Wir sind dankbar für Hinweise auf Schwachstellen und behandeln jede Meldung ernsthaft, vertraulich und zügig. Diese Richtlinie beschreibt, wie Sicherheitsforschende, Kunden und Partner uns Schwachstellen melden können, was sie von uns erwarten dürfen und welche Regeln für eine koordinierte Offenlegung gelten.

Diese Richtlinie gilt für alle Softwareprodukte der UNITEC Informationssysteme GmbH. Sie wird veröffentlicht unter https://www.unitec.de/security sowie über die Datei https://www.unitec.de/.well-known/security.txt.

2. So melden Sie eine Schwachstelle

Meldeweg	Angabe
E-Mail (bevorzugt)	security@unitec.de
Telefon (dringende Fälle)	+49-6181/70118-91 – CRA & Security Team – UNITEC, werktags 8–18 Uhr
Verschlüsselung	PGP – öffentlicher Schlüssel: https://www.unitec.de/security/pgp-key.txt · Fingerprint: F399 46F6 6D2D 766F A04B B09C D2F3 64A5 680B 5351 (Key-ID 0xD2F364A5680B5351).
Sprache	Deutsch; Meldungen auf Englisch werden ebenfalls bearbeitet.

Hilfreiche Angaben in Ihrer Meldung:

- Betroffenes Produkt und Version sowie die Umgebung, in der die Schwachstelle beobachtet wurde,
- nachvollziehbare Beschreibung (Schritte zur Reproduktion, Proof of Concept, Screenshots oder Logauszüge),
- Ihre Einschätzung möglicher Auswirkungen und – falls vorhanden – ein CVSS-Vektor,
- Ihre Kontaktdaten für Rückfragen und Ihren Wunsch zur namentlichen Nennung (optional).

3. Was Sie von uns erwarten dürfen

Zusage	Frist / Inhalt
Eingangsbestätigung	Innerhalb von 3 Werktagen nach Eingang Ihrer Meldung.
Erstbewertung	Wir bewerten Ihre Meldung nach unserem dokumentierten Verfahren und informieren Sie über die Einstufung.
Statusinformation	Wir halten Sie über den Fortschritt der Behebung in angemessenen Abständen auf dem Laufenden.
Behebung und Offenlegung	Wir beheben bestätigte Schwachstellen so schnell wie möglich und stimmen den Zeitpunkt einer etwaigen Veröffentlichung mit Ihnen ab (koordinierte Offenlegung, Zielhorizont: 90 Tage).
Anerkennung	Auf Wunsch nennen wir Sie nach Behebung namentlich in unserem Security Advisory (Hall of Thanks).

4. Spielregeln für die koordinierte Offenlegung

- Geben Sie uns angemessen Zeit zur Behebung, bevor Details veröffentlicht werden (Regelfrist: 90 Tage ab Eingangsbestätigung, einvernehmlich verlängerbar bei komplexen Fällen).
- Nutzen Sie eine gefundene Schwachstelle nur so weit aus, wie es für den Nachweis erforderlich ist.
- Greifen Sie nicht auf fremde Daten zu, verändern oder löschen Sie keine Daten und beeinträchtigen Sie nicht die Verfügbarkeit unserer Systeme oder der Systeme unserer Kunden.
- Kein Social Engineering, kein Phishing, keine physischen Angriffe und keine Angriffe auf Dritte.
- Fordern Sie keine Gegenleistung für die Nichtveröffentlichung von Informationen. Ein Bug-Bounty-Programm besteht derzeit nicht.

5. Safe Harbor – Zusicherung für gutgläubige Sicherheitsforschung

Safe Harbor

Wer sich bei der Suche nach und der Meldung von Schwachstellen in gutem Glauben an diese Richtlinie hält, muss von der UNITEC Informationssysteme GmbH keine zivil- oder strafrechtlichen Schritte befürchten. Wir betrachten regelkonforme Sicherheitsforschung als autorisiert im Sinne dieser Richtlinie und werden keine Anzeige erstatten und keine Schadensersatzansprüche geltend machen. Diese Zusicherung entbindet nicht von der Einhaltung geltenden Rechts und bindet keine Dritten; bei Unsicherheit kontaktieren Sie uns vor weiteren Schritten unter security@unitec.de.

6. Umgang mit Ihren Daten

Wir verwenden Ihre Kontaktdaten ausschließlich zur Bearbeitung der Meldung und zur Abstimmung der Offenlegung. Meldungen werden in unserem Ticketsystem dokumentiert und vertraulich behandelt; technische Details geben wir vor Behebung nur weiter, soweit dies zur Behebung oder aufgrund gesetzlicher Pflichten (z. B. Meldepflichten nach Art. 14 CRA) erforderlich ist.

7. Kontakt

Kontaktstelle	CRA & Security Team – UNITEC
E-Mail	security@unitec.de
Telefon	+49-6181/70118-91
Erreichbarkeit	Werktags 8–18 Uhr (E-Mail- und Telefon-Monitoring); außerhalb der Geschäftszeiten Bereitschaft über das Alarmierungs- und Bereitschaftssystem (Splunk On-Call) mit wechselndem Bereitschaftsrhythmus

8. Änderungshistorie

Version	Datum	Änderung	Autor / Freigabe
1.0	09.09.2026	Ersterstellung	CRA & Security Team

Freigabe

Dieses Dokument wurde geprüft und freigegeben durch die Leitung CRA & Security Team – UNITEC.

Hanau, den 09.09.2026
Ort, Datum

Fynn Scharfenorth
Unterschrift Leitung CRA & Security Team