Responsible Disclosure Policy
der ACSYS Lasertechnik GmbH

ACSYS nimmt die Sicherheit seiner IT-Systeme, Produkte, Maschinensoftware und Dienstleistungen ernst. Wenn Sie eine mögliche Sicherheitslücke gefunden haben, bitten wir Sie um eine vertrauliche Meldung, damit wir diese prüfen, bewerten und geeignete Maßnahmen einleiten können.

Diese Policy beschreibt, wie Sicherheitslücken an ACSYS gemeldet werden können, welches Verhalten wir bei Sicherheitsprüfungen erwarten und wie ACSYS mit gutgläubigen Meldungen im Rahmen einer koordinierten Schwachstellenoffenlegung umgeht.

1. Geltungsbereich

Diese Policy gilt für Sicherheitslücken in:

- öffentlich erreichbaren ACSYS-Websites und ACSYS-Online-Diensten,
- ACSYS-Produkten mit digitalen Elementen,
- ACSYS-Maschinensoftware, Steuerungssoftware, Schnittstellen und Fernwartungskomponenten,
- sonstigen von ACSYS betriebenen oder bereitgestellten IT- oder Produktkomponenten.

Nicht vom Geltungsbereich umfasst sind:

- Kundensysteme, Kundenanlagen, Kundennetzwerke und Produktionsumgebungen von Kunden,
- Systeme, Produkte, Dienste oder Daten von Dritten,
- allgemeine Supportanfragen ohne Sicherheitsbezug,
- rein theoretische Hinweise ohne nachvollziehbaren Bezug zu ACSYS,
- Spam, Phishing-Tests, Social Engineering oder physische Sicherheitsprüfungen,
- Denial-of-Service-Tests, Lasttests oder Störungstests,
- Handlungen, die Daten verändern, löschen, unterdrücken, kopieren, exfiltrieren oder Systeme beeinträchtigen.

Wenn Sie unsicher sind, ob ein Test vom Geltungsbereich umfasst ist, melden Sie die Beobachtung bitte zunächst ohne weitere Prüfung oder Ausnutzung der Schwachstelle.

2. Meldeweg

Bitte melden Sie Sicherheitslücken bevorzugt über das Sicherheitsmeldeformular unter https://www.acsys.de/security-report oder per E-Mail an security@acsys.de.

Sie können eine Meldung ohne Angabe von Name oder Kontaktdaten abgeben. Wenn Sie Kontaktdaten angeben, nutzt ACSYS diese ausschließlich zur Bearbeitung der Sicherheitsmeldung und für Rückfragen. Technische Protokolldaten der Website oder der eingesetzten Plattformen können aus Sicherheits- und Betriebsgründen anfallen.

3. Angaben in der Meldung

Bitte geben Sie möglichst folgende Informationen an:

- betroffenes Produkt, System, Softwareversion, URL oder Komponente,
- kurze Beschreibung der Schwachstelle oder des Sicherheitsvorfalls,
- Schritte zur Reproduktion, soweit dies ohne Schaden und ohne Zugriff auf fremde Daten möglich ist,
- mögliche Auswirkungen und Hinweise auf aktive Ausnutzung, falls bekannt,
- vorhandene Nachweise wie Screenshots, Logauszüge oder technische Details,
- Informationen dazu, ob der Sachverhalt bereits veröffentlicht oder an Dritte gemeldet wurde,
- geplantes Veröffentlichungsdatum und gewünschter Kontaktweg, falls vorhanden.

Bitte übermitteln Sie nur Informationen, die zur Prüfung erforderlich sind. Vermeiden Sie unnötige personenbezogene Daten, Kundendaten, Geschäftsgeheimnisse oder produktionskritische Informationen.

4. Erwartetes Verhalten bei Sicherheitsprüfungen

Bitte handeln Sie gutgläubig, verhältnismäßig und so, dass Schäden vermieden werden. Insbesondere bitten wir Sie:

- Schwachstellen nur so weit zu prüfen, wie es für einen nachvollziehbaren Nachweis erforderlich ist,
- Tests sofort zu beenden, sobald eine Schwachstelle nachvollziehbar belegt ist,
- keine Daten zu verändern, zu löschen, zu unterdrücken, zu kopieren, herunterzuladen oder weiterzugeben,
- keine Zugriffssicherung über den minimal erforderlichen Nachweis hinaus zu umgehen,
- keine Schadsoftware, Ransomware, Persistenzmechanismen, Backdoors oder vergleichbare Werkzeuge einzusetzen,
- keine Denial-of-Service-Angriffe, Lasttests oder Störungstests durchzuführen,
- kein Social Engineering gegen ACSYS, Kunden, Mitarbeitende, Dienstleister oder Partner einzusetzen,
- keine Tests an Kundensystemen, Kundenanlagen, Kundennetzwerken oder Produktionsumgebungen von Kunden durchzuführen,
- eine Schwachstelle nicht weiter auszunutzen, nachdem sie nachgewiesen wurde,
- erlangte Informationen nicht vor einer Abstimmung mit ACSYS öffentlich zu machen.

5. Umgang mit gutgläubigen Meldungen / Safe Harbor

ACSYS begrüßt gutgläubige Sicherheitsmeldungen, die dieser Policy entsprechen.

Wenn Sie eine Sicherheitslücke in gutem Glauben, verhältnismäßig, ohne Schädigungsabsicht und innerhalb des Geltungsbereichs dieser Policy melden, wird ACSYS wegen der bloßen Entdeckung, angemessenen Prüfung und vertraulichen Meldung der Schwachstelle grundsätzlich keine zivilrechtlichen Ansprüche geltend machen und keine Strafanzeige erstatten, soweit keine zwingenden gesetzlichen Pflichten entgegenstehen.

Diese Erklärung gilt nicht für Handlungen außerhalb dieser Policy, insbesondere nicht für:

- Zugriffe auf Kundensysteme, Kundenanlagen, Kundennetzwerke, Produktionsumgebungen, Systeme oder Daten Dritter,
- unbefugte Zugriffe auf fremde oder nicht für Sie bestimmte Daten,
- Veränderung, Löschung, Unterdrückung, Kopie, Exfiltration oder Weitergabe von Daten,
- Beeinträchtigung, Störung oder Sabotage von Systemen, Diensten, Maschinen oder Produktionsumgebungen,
- Einsatz oder Verbreitung von Schadsoftware, Persistenzmechanismen oder Backdoors,
- Denial-of-Service-Angriffe, Lasttests oder Störungstests,
- Umgehung von Zugriffsschutz über den minimal erforderlichen Nachweis hinaus,
- Social Engineering, Phishing, Identitätstäuschung, Erpressung oder Drohung,
- Forderung einer Vergütung oder Veröffentlichung unter Druck,

ACSYS Lasertechnik GmbH
Leibnizstraße 9
70806 Kornwestheim
Deutschland

T: +49 7154 808 75 0
F: +49 7154 808 75 19
E: info@acsys.de
W: www.acsys.de

Geschäftsführer:
Gerhard Kimmel, Sascha König
Amtsgericht Stuttgart HRB 206629
St.-Nr. 71300/09208
USt.-IdNr. DE813681276

VR-Bank Ludwigsburg eG
IBAN: DE77604914300304670006 / BIC: GENODES1VBB
Commerzbank AG
IBAN: DE37600400710521819300 / BIC: COBADEFFXXX
Deutsche Bank AG Ludwigsburg
IBAN: DE08604700820019111400 / BIC: DEUTDESS604

- Veröffentlichung oder Weitergabe von Informationen vor Abstimmung mit ACSYS.

Diese Policy stellt keine allgemeine Erlaubnis zum Zugriff auf ACSYS-Systeme, ACSYS-Produkte, Kundensysteme, Drittsysteme oder Daten Dritter dar. ACSYS kann keine Straffreiheit zusichern und kann Entscheidungen von Strafverfolgungsbehörden, Kunden oder anderen Dritten nicht beeinflussen.

6. Umgang mit Ihrer Meldung

ACSYS prüft eingehende Sicherheitsmeldungen risikoorientiert. Wenn Kontaktdaten angegeben wurden, kann ACSYS den Eingang bestätigen und Rückfragen stellen.

Je nach Art und Schwere der Meldung kann ACSYS:

- technische Prüfungen durchführen und betroffene Produkte, Systeme oder Komponenten bewerten,
- Korrektur- oder Minderungsmaßnahmen einleiten,
- betroffene Nutzer oder Kunden informieren,
- gesetzlich erforderliche Meldungen an zuständige Behörden oder Koordinierungsstellen abgeben,
- eine koordinierte Veröffentlichung vorbereiten.

ACSYS gibt keine feste Bearbeitungsdauer für alle Fälle ab. Kritische oder aktiv ausgenutzte Schwachstellen werden priorisiert behandelt.

7. Koordinierte Veröffentlichung

Bitte veröffentlichen Sie Informationen zu einer gemeldeten Schwachstelle erst nach Abstimmung mit ACSYS oder nachdem eine angemessene Korrektur- oder Minderungsmaßnahme verfügbar ist.

Wenn Sie eine Veröffentlichung planen, teilen Sie ACSYS bitte frühzeitig das geplante Veröffentlichungsdatum und den geplanten Inhalt mit. ACSYS wird eine koordinierte Veröffentlichung unterstützen, soweit dadurch die Sicherheit von ACSYS, Kunden, Nutzern oder Dritten nicht gefährdet wird.

ACSYS behält sich vor, Informationen zurückzuhalten oder nur eingeschränkt zu teilen, wenn eine Veröffentlichung die Ausnutzung der Schwachstelle erleichtern oder die Sicherheit von ACSYS, Kunden, Nutzern oder Dritten gefährden könnte.

8. Kein Bug-Bounty-Programm

ACSYS betreibt derzeit kein Bug-Bounty-Programm und sagt keine Vergütung für gemeldete Schwachstellen zu. Eine Meldung begründet keinen Anspruch auf Vergütung, Auftragserteilung, Anerkennung oder Veröffentlichung.

9. Datenschutz und Vertraulichkeit

ACSYS behandelt Sicherheitsmeldungen vertraulich. Personenbezogene Daten werden nur verarbeitet, soweit dies für die Prüfung, Bearbeitung, Rückfragen, Sicherheitsmaßnahmen oder gesetzliche Pflichten erforderlich ist.

Bitte übermitteln Sie keine unnötigen personenbezogenen Daten, Kundendaten, Geschäftsgeheimnisse oder produktionskritischen Informationen. Wenn solche Informationen versehentlich übermittelt werden, kann ACSYS deren Löschung, Einschränkung oder gesonderte Behandlung vornehmen.

10. Kontakt

ACSYS Security Team
https://www.acsys.de/security-report
security@acsys.de

Stand: 08/2026