Vulnerability Disclosure Policy



Document Owner: Uladzimir Pashkevich, Head of IT Security

Reviewed: Nov 24, 2026 , Version 1.0

Scope 3
Report a Vulnerability 3
Responsible Security Research 4
What to Expect 4
Applicability of the Cyber Resilience Act 5

REGULA welcomes responsible, good-faith reports of suspected security vulnerabilities in our products and services. We aim to investigate reported issues, reduce risks to users, and coordinate appropriate remediation and disclosure.

Scope

This policy covers REGULA-developed or maintained software and firmware, including **Regula Document Reader SDK**, **Regula Face SDK**, **Regula IDV Platform**, REGULA-operated services, **regulaforensics.com** and its subdomains, and **explore.regula.app**. Reports about third-party components that may affect REGULA products are also welcome.

Customer-managed deployments and systems owned by other parties are not authorized testing targets under this policy. Reports affecting older or unsupported versions are welcome, but reporting an issue does not extend their support period.

Report a Vulnerability

Send suspected security vulnerabilities to vulnerabilities@regulaforensics.com. A customer account is not required.

If possible, include the affected product and version, configuration, a description of the security impact, minimal steps to reproduce the issue, and sanitized supporting evidence. We accept incomplete reports and do not require a working exploit.

Do not email passwords, access tokens, customer identity documents, biometric information, or unnecessary personal data. If sensitive evidence is needed, request an approved secure transfer method first. Clearly flag any suspected active exploitation or ongoing security incident.

For ordinary technical support, use support@regulaforensics.com.

Responsible Security Research

Use your own or explicitly authorized test environment and synthetic data. Obtain **written authorization before testing REGULA-operated live services** or any environment you do not control. This policy is not blanket permission to test websites, bypass licenses, or access customer environments.

Do not conduct denial-of-service or high-volume testing, social engineering, physical attacks, deploy malware, establish persistence, or access, copy, change, or disclose another person's data. If you inadvertently encounter sensitive data, stop and notify us promptly.

This policy does not establish a paid bug bounty program or grant legal immunity.

What to Expect

REGULA acknowledges reports without undue delay, evaluates their impact and affected versions, and coordinates investigation and remediation with the responsible teams. We may request additional details and will communicate material updates where contact information is available.

We support coordinated disclosure and ask researchers to allow a reasonable opportunity to investigate and protect affected users before publishing details that could facilitate exploitation. Public security information and relevant fixes are communicated through product release notes at **https://docs.regulaforensics.com/**. Where

appropriate, we coordinate CVE assignment with the responsible CVE Numbering Authority.

Urgent security incidents and legally required customer or regulatory notifications are handled separately and are not delayed by routine publication schedules.

Applicability of the Cyber Resilience Act

For events within the scope of Article 14 of the Cyber Resilience Act, the reporting clock runs from the applicable point of awareness, not completion of root-cause analysis. Regulatory notifications are submitted through the CRA Single Reporting Platform to the designated CSIRT coordinator and ENISA as required.

Reporting on an actively exploited vulnerability involves an early warning within 24 hours of receiving the information; a vulnerability notification within 72 hours; and a final report no later than 14 days after the availability of corrective or mitigating measures.

Reporting on a serious incident affecting product security involves an early warning within 24 hours of receiving the information; an incident notification within 72 hours; and a final report within one month of the incident notification, with appropriate progress reporting procedures applied if the handling process is still ongoing.

Not every scanner finding or CVE triggers Article 14; the statutory criteria must be assessed and the decision documented. Impacted users must be informed without undue delay where required, including available protection measures. Publishing Release Notes or a CVE does not replace mandatory customer or regulatory notification.

Other applicable privacy, contractual and regulatory notification duties remain governed by the Incident Response Plan and the relevant legal requirements. Uncertainty about

the complete impact must not prevent an initial report where the reporting threshold has already been met.