FREE GUIDE

5 Things to Have Ready Before Your First Vulnerability Report

One day, a stranger will email you about a security flaw in your product. A plain-English guide to being ready before that day.

If you ship software, one day a security researcher (or a customer, or a stranger on the internet) will tell you about a flaw in it. That email is not an attack; it's a gift with awkward wrapping. Teams that prepared handle it in days and earn trust. Teams that didn't often make it worse in the first reply. Here are the five things to have ready before it arrives.

A free guide from Sylvan Assurance — plain-English security, without us ever seeing your data.

1. An address where reports can actually reach you

Researchers give up quickly when there's no obvious way to report. The fix costs nothing: a security@yourcompany.com mailbox that a real person reads, and a /security page (or a security.txt file) saying "found something? tell us here." If the report can't reach you, your first notice may be a public post instead.

2. A short vulnerability disclosure policy

One page, plain English: we welcome reports, here's where to send them, and here's what we'll do and roughly when. And we won't take legal action against good-faith research. That last sentence matters more than any other. It's the difference between researchers telling you quietly and telling the world. (This is a policy you can write in an afternoon from a template.)

3. A triage habit: assess before you answer

The first instinct is either panic or dismissal. Both show up in the first reply, and both are expensive. The prepared version is a simple habit: acknowledge receipt quickly (a day is fine), then assess before promising anything. Three questions cover most triage: is it real, what could someone actually do with it, and is anyone doing that now?

4. A path from "confirmed" to "fixed and shipped"

A confirmed flaw needs an owner, a priority, and a route into your normal release process. That routing gets decided now, not negotiated during the incident. The question to answer in advance: when a real security fix competes with the feature roadmap, who decides, and how fast can an emergency release actually go out?

5. A thank-you, and a straight answer

Researchers mostly want two things: acknowledgement and a fix. Thank them, keep them posted, credit them if they want it (a simple acknowledgements page costs nothing). And when customers ask what happened, a short, honest account beats a polished non-answer every time. Trust is built in exactly these moments.

The honest summary

A reachable address, a one-page policy, an assess-first habit, a pre-agreed fix path, and basic courtesy. None of it requires a security team. Having it ready turns one of the scariest emails a founder can receive into a routine Tuesday.

Where to go from here

The free PSIRT (Product Security Incident Response Team) readiness assessment scores how prepared you are to receive and handle vulnerability reports. It covers governance, technical, and communication readiness, entirely in your browser.

When you're ready for the working runbooks, communication templates, and regulatory decision trees, the PSIRT Response toolkit lays them out. It's from $49, one-time, with a 30-day money-back guarantee.

Take the free assessment: sylvanassurance.com/free/psirt/

See the full toolkit: sylvanassurance.com/psirt-response.html

Scan for the free assessment that goes with this guide.
sylvanassurance.com/go/free-psirt-response