Third Party Security Checklist

No matter how hard you work to secure your applications and data, every third party with which you share data can open up a new attack vector.

Making sure third parties treat your sensitive data appropriately, and generally adhere to security best practices, will reduce the likelihood of a breach. Use this checklist as one way to assess the security standards of the third parties you work with before sharing data with them.

This is our truncated version of the robust VSA Questionnaire, a collaborative effort of their working group.

☐ **AUTHENTICATION**

Find out about policies governing passwords, remote connection to production systems, multi-factor authentication (MFA), SSO/SAML for customer access.

☐ **DATA ACCESS**

Understand who will access your data, rules in relation to role provisioning, deprovisioning, and recertification, and how sensitive data is stored.

☐ **PROACTIVE SECURITY**

Discover their security testing cadence (periodic, or continuous as with a bug bounty program), if they have a vulnerability disclosure policy, what the remediation cadence to patch/update is, and if they have an established bug bounty program.

☐ **API MANAGEMENT**

Be sure they secure their API tier by understanding their policies for:

- API rate limiting
- API key storage
- IP whitelisting for API access
- API user authentication

☐ **ENCRYPTION**

Determine the data encryption standard they use and how they encrypt customer data.

☐ **STAFF, POLICIES, AND TRAINING**

- Do they have an Information Security Program (InfoSec SP) and information security risk management program (InfoSec RMP) in place?
- What types of management, leadership, and security staff forums are in place?
- Get comfortable with their policies on background checks, confidentiality agreements, procedures for deactivating access upon termination or departure.

☐ **INDUSTRY STANDARDS**

Do information security and privacy policies align with industry standards (ISO-27001, NIST Cyber Security Framework, ISO-22307, CoBIT, etc.)?

☐ **ENDPOINT SECURITY**

Understand their policies for user devices and servers.

Do they follow configuration management best practices for servers and network devices?

How are cryptographic keys (key management system, etc) managed?

Determine their threat monitoring, communication, and response processes.

About HackerOne

HackerOne is the #1 hacker-powered security platform. More than 1,000 organizations, including the U.S. Department of Defense, General Motors, Google Play, Twitter, GitHub, Nintendo, Panasonic Avionics, Qualcomm, Starbucks, and Dropbox, trust HackerOne to find critical software vulnerabilities.