Vulnerability Disclosure Policy

Effective Date: March 25, 2025

1. Introduction

Staples is committed to ensuring the security of our customers and the information they share with us via our online platforms and services. We also recognize the valuable efforts that security researchers play in highlighting cybersecurity vulnerabilities and concerns. The purpose of this policy is to provide clear guidelines for conducting vulnerability discovery activities and to convey how to submit discovered vulnerabilities.

2. Compliance

If you act in good faith and adhere to this policy, Staples commits to not pursuing legal action or referring the matter to law enforcement. Any ambiguities will be resolved in favor of security researchers acting ethically and responsibly.

3. Requirements

This policy requires that you:

- Notify us as soon as possible after you discover a real or potential security issue;
- Make every effort to avoid privacy violations, degradation of user experience, disruption to systems and destruction or manipulation of data;
- Only use exploits to the extent necessary to confirm a vulnerability's presence — do not use an exploit to collect, modify or delete data, establish persistent access or access and/or test other systems, networks or applications; and
- Do not disclose the details of any alleged vulnerability to third parties without express written consent from Staples — unauthorized disclosure will deem the submission as noncompliant with this policy.

Once you've established that a vulnerability exists or encounter any confidential or sensitive data (including personal information, financial information, or proprietary information), **you must stop your test, notify us immediately and not disclose this data to anyone else**.

4. Test Methods

The following test methods are not authorized:

- Denial of service (DoS or DDoS) tests or other tests that stress-test or have the potential to impair access to or damage systems, networks, applications or data, even if temporarily
- Accessing, downloading or modifying data residing in an account that does not belong to you
- Testing in a manner that would result in sending unsolicited or unauthorized junk mail, spam, e-mail notices, phone calls, text messages or other forms of unsolicited messages to other parties — including Staples associates, customers or partners
- Social engineering, including but not limited to misrepresenting Staples or its personnel
- Trespassing or other tests with a physical security aspect
- Posting, transmitting, uploading, linking to, sending or storing any malicious software
- Testing third-party systems, networks, applications, and services, even if operated on behalf of Staples

5. Scope

This policy applies to the following Staples family websites and services:

- Staples.com
- StaplesConnect.com
- StaplesAdvantage.com
- StaplesPromotionalProducts.com
- Quill.com
- HiTouchBusinessServices.com
- ediversitynetwork.com
- SouthwestOrdering.com
- app.staplespay.com

Testing under this policy is strictly limited to the web applications listed above. Network infrastructure, internal systems, and third-party services (including cloud environments) are out of scope. If you believe a security issue exists outside the defined scope that affects Staples, please contact us at vulnerabilityreport@staples.com before conducting any testing.

We may update this scope over time, and we encourage researchers to check back periodically for changes.

6. Reporting a Vulnerability

We accept vulnerability reports via email to vulnerabilityreport@staples.com. Reports may be submitted anonymously.

What we would like to see from you

In order to help us triage and prioritize submissions, we recommend that your report:

- Describes full details of the vulnerability and its location;
- Provides step-by-step instructions for us to be able to validate and reproduce the finding; and
- Includes any proof of concept scripts or resulting artifacts, such as screen captures.

What you can expect from us

If you submit a valid security vulnerability in compliance with this policy, we will:

- Acknowledge the receipt of the report within 5 business days;
- Communicate with you to understand and validate the issue as necessary; and
- Address the submitted vulnerability as appropriate, as deemed by Staples.

Note that Staples does not operate a bug bounty program and we make no offer of compensation in exchange for submitting potential issues.

Staples may modify the terms of this policy or terminate this policy at any time.

7. Questions

If you are in doubt about the scope, acceptable test methods or any other provisions of this policy, you are encouraged to contact us first at vulnerabilityreport@staples.com. We also invite you to contact us with suggestions for improving this policy.