Vulnerability Disclosure Policy

Version:	2.1
Date of version:	3/28/2022
Created by:	Slawomir Zabkiewicz (VP of Engineering)
Approved by:	VP of Engineering
Confidentiality level:	Tier 3-Public Data

Change history

Date	Version	Created by	Description of change
11/20/2020	1.0	Slawomir Zabkiewicz	Policy created.
11/01/2021	2.0	Slawomir Zabkiewicz	Annual review, added changelog, versioning, confidentiality level and footer. Updated scope.
3/28/2022	2.1	Greg Fowl	Updated to exclude Marketing website from scope, periodic review, language clean-up.

1. Purpose

Maintaining the security of our products is a high priority of TINT. This Vulnerability Disclosure Policy (VDP) is intended to provide a clear channel for the security research community to provide vulnerability disclosures to the TINT Team.

Our hope is to foster an open relationship with the security community, as we recognize the importance of application and data security and look to the security community to help ensure we are meeting the highest levels for the benefit of our customers and partners. We have developed this policy to publicly demonstrate our commitment to security as a key value and to uphold our legal responsibility to good-faith security researchers who choose to help validate our applications.

If you believe you have found a security vulnerability that could impact TINT, or our customers and their users, we encourage you to report this right away. We will investigate all legitimate reports and resolve any confirmed vulnerabilities in a timely manner. We ask that you follow this policy and make a good faith effort to avoid privacy violations, destruction of data, and interruption or degradation of our service during your research.

2. Scope

Services that TINT provides or any TINT product are in scope, including:

- www.tintup.com
- api.tintup.com
- cdn.hypemarks.com
- *.tintpages.com

Any services not expressly listed above, such as any connected services, are excluded from scope and are not authorized for testing. Additionally, vulnerabilities found in non-TINT systems from our vendors fall outside of this policy's scope and should be reported directly to the vendor according to their disclosure policy (if any). If you aren't sure whether a system or endpoint is in scope or not, contact us at security@tintup.com before beginning your research.

The following activities/conditions are **out of scope** for the Vulnerability Disclosure Program.

- futureofmarketing.tintup.com and gallery.tintup.com
- For www.tintup.com and cdn.hypemarks.com, anything that falls outside of /t/*, /p/*, /mix/*, /terms/*, /app/*, /dist/*, /templates/*, /login, /logout, /analytics/*, /right_requests/terms/*, /public_post_terms/*, /hootsuite/*, /external/*, /themes/*, /launchpad/*, and /raw/*
- For api.tintup.com, anything under /v1/ that isn’t documented at https://developers.tintup.com/v1/
- User interface bugs or typos.
- Missing Best Practice, Configuration or Policy Suggestions.
- Any Denial of Service (DoS) attack against TINT and our products.

- Physical attacks against TINT employees, offices, and data centers.
- Social engineering of TINT employees, contractors, vendors, or service providers.
- Knowingly posting, transmitting, uploading, linking to, or sending any malware.
- Pursuing vulnerabilities which send unsolicited bulk messages (spam) or unauthorized messages.

3. Authorization

If you make a good faith effort to comply with this policy during your security research, we will consider your research to be authorized. We will work with you to understand and resolve the issue quickly, and TINT will not recommend or pursue legal action related to your research. Should legal action be initiated by a third party against you for activities that were conducted in accordance with this policy, we will make this authorization known.

4. Guidelines

TINT 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 production 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 compromise or exfiltrate data, establish persistent command line access, or use the exploit to pivot to other systems.
- Do not submit a high volume of low-quality reports.

Once you've established that a vulnerability exists or you encounter any sensitive data (including personally identifiable information, financial information, or proprietary information or trade secrets of any party), you must stop your test.

5. Test Methods

The following test methods are not authorized:

- Network denial of service (DoS or DDoS) tests or other tests that impair access to or damage a system or data
- Physical testing (e.g. office access, open doors, tailgating), social engineering (e.g. phishing, vishing), or any other non-technical vulnerability testing

6. Reporting a Vulnerability

TINT accepts and discusses vulnerability reports via email at security@tintup.com.

In order to help us triage and prioritize submissions, we ask that your reports:

- Describe the location the vulnerability was discovered and the potential impact of exploitation.

- Offer a detailed description of the steps required to reproduce the vulnerability, including screenshots and proof of concept (POC) scripts/code. Please use extreme care to properly label and protect any exploit code.
- Be in English, if possible.

Please note that results from automated scanning tools will not be accepted.

If your report includes sensitive information, please visit https://www.tintup.com/security/pgp-key.txt to obtain our public PGP key so that you can use to encrypt your email/report.

When you choose to share your contact information with us, we commit to coordinating with you as openly and as quickly as possible:

- Within 5 business days, we will acknowledge that your report has been received.
- To the best of our ability, we will confirm the existence of the vulnerability to you and be as transparent as possible about what steps we are taking during the remediation process, including on issues or challenges that may delay resolution.
- We will maintain an open dialogue to discuss issues.

7. Disclosure

In order to protect our customers, TINT requests that you not post or share any information about a potential vulnerability in any public setting until we have researched, responded to, and addressed the reported vulnerability and informed customers if needed.

8. Bounties

The decision to pay a reward is entirely at our discretion. You must not violate any law. You are responsible for any tax implications or additional restrictions depending on your country and local law. We reserve the right to cancel this program at any time.