RESPONSIBLE DISCLOSURE POLICY

2020/06/12	Version 1.0

TABLE OF CONTENTS

POLICY

Markforged takes protecting our customers' data seriously and that starts with being transparent about our security practices. Providing a method for security researchers to responsibly report vulnerabilities is essential for that transparency.

REPORTING

If you believe you have found a security vulnerability related to Eiger, Markforged hardware, or the Markforged website, please let us know. We will investigate legitimate reports and do our best to fix valid issues.

Your report should include a detailed description of your discovery with clear, concise, reproducible steps or a working proof-of-concept. Please refrain from requesting compensation for reporting vulnerabilities as it is Markforged's policy not to pay. You can submit your report by emailing responsible-disclosure@markforged.com.

VULNERABILITY DISCLOSURE

Your report will be sent to the Markforged Security team, and will remain non-public while it is investigated. Once a report has been validated a decision will be made by the Markforged Security team regarding whether the vulnerability will be made public. Public vulnerabilities related to Eiger may be published on the Eiger status page.

To promote the discovery and reporting of vulnerabilities and increase user safety, we ask that you:

- Share the security issue with us in detail;
- Please be respectful of our existing applications. Spamming forms through automated vulnerability scanners is explicitly out of scope;
- Do not access or modify our data or our users' data, without explicit permission of the owner. Only interact with your own accounts or test accounts for security research purposes;
- Contact us immediately if you do inadvertently encounter user data. Do not view, alter, save, store, transfer, or otherwise access the data, and immediately purge any local information upon reporting the vulnerability to Markforged;
- Act in good faith to avoid privacy violations, destruction of data, and interruption or degradation of our services (including denial of service); and
- Otherwise comply with all applicable laws.

We will not negotiate in response to duress or threats (e.g. we will not pay a bounty under threat of withholding the vulnerability or threat of releasing the vulnerability or any exposed data to the public). Markforged does not provide compensation for vulnerability reports.

IN SCOPE

Target	**Eligible**	**Ineligible**
Eiger	eiger.io	
Markforged website	markforged.com	*.markforged.com
Markforged hardware	First-party hardware: ● 3D Printers ○ Mark 2 ○ Onyx Pro ○ Onyx One ○ X3 ○ X5 ○ X7 ○ Metal X ● Furnaces ○ Sinter-1 ○ Sinter-2 ● Wash stations ○ Wash-1	Third-party hardware

OUT OF SCOPE VULNERABILITIES

- Clickjacking on pages with no sensitive actions
- Cross-Site Request Forgery (CSRF) on unauthenticated forms or forms with no sensitive actions
- Attacks requiring MITM or physical access to a user's device.
- Previously known vulnerable libraries without a working Proof of Concept.
- Comma Separated Values (CSV) injection without demonstrating a vulnerability.
- Missing best practices in SSL/TLS configuration.
- Any activity that could lead to the disruption of our service (DoS).
- Content spoofing and text injection issues without showing an attack vector/without being able to modify HTML/CSS

- Rate limiting or bruteforce issues on non-authentication endpoints
- Missing best practices in Content Security Policy.
- Missing HttpOnly or Secure flags on cookies
- Missing email best practices (Invalid, incomplete or missing SPF/DKIM/DMARC records, etc.)
- Vulnerabilities only affecting users of outdated or unpatched browsers [Less than 2 stable versions behind the latest released stable version]
- Software version disclosure / Banner identification issues / Descriptive error messages or headers (e.g. stack traces, application or server errors).
- Public Zero-day vulnerabilities that have had an official patch for less than 1 month will be awarded on a case by case basis.
- Tabnabbing
- Open redirect - unless an additional security impact can be demonstrated
- Issues that require unlikely user interaction

MODIFICATION

We may modify the terms of this program or terminate this program at any time.

OWNERSHIP AND REVIEW

This document is owned by the Markforged Security Team.
This document shall be reviewed on an annual basis.
Changes to this document shall be in accordance with the *ISMS Document and Records Control Standard*.

RESPONSIBLE DISCLOSURE POLICY	
2020/06/12	Version 1.0

Document Properties

Property	Description
Circulation	Public
Document Owner	Markforged Security Team
Next Scheduled Review	2020/06/12

Document Approvals

Approver Name	Title	Date
David Benhaim	CTO	2020/06/12
Markforged Security Team	Various	2020/06/12

Revision History

Version	Date	Description of Changes	Revised by
1.0	2020/06/12	Initial Version	Markforged Security Team