# Vulnerability Disclosure Policy

## I. Introduction

***AmTrust Financial Services, Inc.***, our subsidiaries, and affiliates (collectively, "AmTrust", "we", "us" or "our") is committed to a strong information governance program and endeavors to protect customer and website user information. A part of this process is continuous review and improvement of our security posture. This Vulnerability Disclosure Policy (the "Policy") is intended to give security researchers clear guidelines for conducting vulnerability discovery activities and to convey the requirements to submit information of discovered vulnerabilities. If you believe you've found a new security vulnerability in one of our products or platforms, please follow the Guidelines below and notify us by emailing ***SecurityVDP@amtrustgroup.com***.

We take the security of our systems seriously and value the role that independent security researchers play. The disclosure of security vulnerabilities helps ensure the security and privacy of our users. This Policy governs how to review and report a security vulnerability; please review this Policy before testing and/or reporting a vulnerability. This Policy describes what systems and types of research are covered, how to send us vulnerability reports, and how long we ask security researchers to wait before publicly disclosing vulnerabilities.

We want security researchers to feel comfortable reporting vulnerabilities they've discovered - as set out in this Policy - so we can fix them and protect our users. We have developed this Policy to reflect our values and uphold our sense of responsibility to security researchers who share their expertise with us in good faith. We encourage you to contact us to report potential vulnerabilities in our systems.

## II. Authorization

By complying with this Policy, we will consider your research to be authorized, we will work with you to understand and resolve the issue, and AmTrust will not recommend or pursue legal action directly related to your research. We will investigate legitimate reports and make every effort to quickly correct any vulnerability. 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.

## III. Responsible Disclosure Guidelines

1. **We require that all researchers:**
   - Make every effort to avoid privacy violations, degradation of user experience, disruption to production systems, and destruction of data during security testing.
   - Perform research only within the scope set out in this Policy. For example, we expect researchers to provide details of the vulnerability, including information needed to reproduce and validate the vulnerability and a Proof of Concept (POC)
   - Use the identified communication channels to report vulnerability information to us.
   - Keep information about any vulnerabilities you've discovered confidential between yourself and AmTrust.
2. **If you follow the requirements documented in this Policy we shall:**
   - Consider a good faith security researcher not to have violated the Computer Fraud and Abuse Act, and we will not bring a copyright enforcement action under the Digital Millennium Copyright Act.
   - Respond in a timely manner, acknowledging receipt of your vulnerability.

- If possible, depending on the facts and circumstances, provide an estimated time frame for addressing the vulnerability report and notify you when the vulnerability has been fixed.
- Recognize your contribution on our ***AFSI Security Researcher Hall of Fame*** (see below) if you are the first to report the issue, the issue is not a known issue, and we make a code or configuration change based on the issue.

**3. AmTrust does not permit the following:**

- Performing actions that may negatively affect AmTrust or its users (e.g. Spam, Brute Force, Denial of Service, etc.).
- Conducting vulnerability testing of participating services using anything other than test accounts.
- Violating any laws or breaching any agreements in order to discover vulnerabilities.
- Destroying or corrupting, or attempting to destroy or corrupt, data or information that does not belong to you.
- Accessing, or attempting to access, data or information that does not belong to you.
- Findings from physical testing such as office access (e.g. open doors, tailgating).
- Findings derived primarily from social engineering (e.g. phishing, vishing).
- Findings from third party applications or third-party systems.
- UI and UX bugs and spelling mistakes.
- Network level Denial of Service (DoS/DDoS) vulnerabilities.

**4. Things we do not want to receive:**

- Personally identifiable information (PII).
- Credit card holder data.
- Informational vulnerabilities.

**5. How to report a security vulnerability?**

Send any vulnerability information by emailing ***SecurityVDP@amtrustgroup.com***. Please include the following details with your report:

- Description of the location, data, and potential impact (if known) of the vulnerability.
- A detailed description of the steps required to reproduce the vulnerability (POC scripts, screenshots, and compressed screen captures are all helpful).
- Your name/handle and a link for recognition in our Hall of Fame, if that is desired.

## IV. AmTrust Security Researcher Hall of Fame

We appreciate and want to recognize the contributions of security researchers. If you are the first researcher to report a confirmed vulnerability, we will list your name in our Hall of Fame (unless you would prefer to remain anonymous). You must comply with this Policy to be considered.