STATE OF DELAWARE
DEPARTMENT OF TECHNOLOGY AND INFORMATION
801 Silver Lake Blvd.
Dover, Delaware 19904

Doc Ref Number:	SE-VUL-001	**Revision Number:** 0
Document Type:	Enterprise Policy	**Page:** 1 of 8
Policy Title:	Vulnerability Disclosure Policy	

Synopsis:	Guide collaboration between the public and DTI regarding reported vulnerabilities.		
Authority:	Title 29 Chapter 90C Delaware Code, §9004C – General Powers, duties and functions of DTI "2) Create, implement and enforce statewide and agency technology solutions, policies, standards and guidelines, including as recommended by the Technology Investment Council on an ongoing basis and the CIO"		
Applicability:	This Policy is applicable to all users of the State of Delaware communications and computing resources.		
Effective Date:	6/26/2018	**Expiration Date:**	None
POC for Changes:	Solomon Adote, Chief Security Officer		
Approval By:	James Collins, Chief Information Officer		
Approved On:	6/26/2018		
Review Date:	6/26/2018		

TABLE OF CONTENTS

1. Policy

POLICY STATEMENT

Purpose

To provide visitors to State of Delaware websites a way to report potential security vulnerabilities. The delaware.gov website includes *Report a Vulnerability* link.

Scope

- This policy does not provide any third party right of action or create any third party beneficiary.
- Any public-facing website owned, operated, or controlled by the State of Delaware, including web applications hosted on those sites.
- The following test types are not authorized:
  - Network or application denial of service (DoS or DDoS)

- Physical (e.g. office access, open doors, tailgating), social engineering (e.g. phishing, vishing), or any other non-technical vulnerability
- Brute-forcing a login page via *any conceivable method*, including the enlistment of computing system
- Infrastructure vulnerabilities, including:
  - DNS issues (i.e. DNS MX records, SPF records, etc.)
  - Server configuration issues (i.e., open ports, TLS, etc.)
  - ARP spoofing/session highjacking
- Clickjacking
- Active scanning or automated tools
- LDAP Injection

How to Submit a Vulnerability Report

If website visitors wish to submit a vulnerability report they shall use the *Report a Vulnerability* link on https://delaware.gov. A form will be presented to securely capture details of the discovered vulnerability. The submitter should include clear, concise and reproducible steps.

Confidentiality

Any vulnerability reports, investigations, and communications or records related thereto, are confidential and exempt from disclosure pursuant to the Delaware Freedom of Information Act ("FOIA," Chapter 100 of Title 29 of the Delaware Code) to extent permissible by law.

Guidelines

DTI agrees not to pursue claims against those who disclose potential vulnerabilities to this policy where the contributor:

- Provides a summary of sufficient detail to reproduce the vulnerability, including the target, steps, tools, and artifacts used during discovery;
- Does not cause harm to State of Delaware, Delaware residents, or others;
- Does not initiate a fraudulent financial transaction;
- Does not intentionally store or otherwise compromise or destroy State of Delaware data;
- Does not intentionally cause damage to State of Delaware systems or applications nor cause related processes to malfunction;
- Does not compromise the privacy or safety of Delaware residents, customers and the operation of our services;
- Does not violate any federal, state, or local law or regulation; and
- Does not publicly disclose vulnerability details without State of Delaware written permission.

Your Responsibilities

This Vulnerability Disclosure Policy sets out expectations when working with good-faith testers, as well as what to expect from the State . To encourage good-faith security testing and disclosure of discovered vulnerabilities, the contributor shall fulfill the following responsibilities:

- Make a good faith effort to avoid privacy violations and disruptions to others, including, but not limited to, unauthorized access to or destruction of data and interruption or degradation of our services.

- Do not exploit a security issue you discover for any reason. This includes demonstrating additional risk, such as attempted compromise of sensitive company data or probing for additional issues.

- Do not intentionally violate any other laws or regulations, including, but not limited to, laws and regulations prohibiting the unauthorized access to data.

- If contributor inadvertently cause a privacy violation or disruption (such as accessing account data, service configurations, or other confidential information) while investigating an issue, data is prohibited from being saved, stored, transferred or otherwise further accessed after initial discovery. You shall notify the State of Delaware of such privacy violation or disruption as soon as possible. A written description of the vulnerability or a screenshot demonstrating the existence of the vulnerability may need to serve as an acceptable form of proof.

State of Delaware Responsibilities

- Information submitted to the State of Delaware under this policy will be used to mitigate or remediate vulnerabilities and improve our cyber defenses.

- The State will take vulnerability reports seriously. The State will investigate disclosures and strive to ensure that appropriate steps are taken to mitigate the risk and remediate reported vulnerabilities.

- The State will process reports and may contact you if more information is needed.

- The State will not commit to a remediation or response time.

2. Definitions

ARP (Address Resolution Protocol) - A network layer protocol used to convert an IP address into a physical address.

ARP Spoofing -A method of attacking an Ethernet LAN by updating the target computer's ARP cache with both a forged ARP request and reply packets in an effort to change the Layer 2 Ethernet MAC address.

Clickjacking - A technique used by an attacker to collect an infected user's clicks.

Content Spoofing/Text Injection - A type of exploit used by an attacker to present a fake or modified web site to the user as if it were legitimate.

CSRF (Cross-site Request Forgery) - A type of malicious exploit of a website where unauthorized commands are transmitted from a user that the website trusts. Unlike cross-site scripting (XSS), which exploits the trust a user has for a particular site, CSRF exploits the trust that a site is in a user's browser.

DNS (Domain Name System) - The Domain Name System is a hierarchical decentralized naming system for computers, services, or any resource connected to the Internet or a private network.

DNS MX Record - The 'mail exchange' record that indicates how email messages should be routed.

DNS SPF Record - The Sender Policy Framework record is used to indicate to mail exchanges which hosts are authorized to send mail for a domain.

DoS (Denial of Service) and DDoS (Distributed Denial of Service) - An attack where the attackers send excessive messages to prevent legitimate users from using the service.

LDAP – Lightweight Directory Access Protocol is an open, vendor-neutral, industry standard application protocol for accessing and maintaining distributed directory information services over an Internet Protocol (IP) network.

LDAP Injection - An attack used to exploit web based applications that construct LDAP statements based on user input.

Social Engineering - The use of deception to manipulate individuals into divulging confidential or personal information that may be used for fraudulent purposes.

TLS (Transport Layer Security) - A protocol that guarantees privacy and data integrity between client/server applications communicating over the Internet.

Phishing - The attempt to acquire sensitive information such as usernames, passwords, and credit card details by masquerading as a trustworthy entity.

Self-XSS - A social engineering attack used to gain control of victims' web accounts, most commonly Facebook accounts.

Vishing - The practice of using social engineering over the telephone system to gain access to private personal and financial information from the public for an illicit purpose.

Vulnerability - A set of conditions that leads to a failure of the confidentiality, integrity, or availability of an information system. Examples of a vulnerability may include any of the following:

- Executing commands as another user;
- Accessing data in excess of specified or expected permission;
- Posing as another user or service within a system;
- Inadvertently or intentionally destroying data without permission;
- Exploiting an encryption implementation weakness that significantly reduces the time or computation required to recover the plaintext from an encrypted message.

3. Development and Revision History

Initial version established – June 26, 2018

4. Approval Signature Block

Name & Title: State Chief Information Officer	**Date**

5. Related Policies and Standards

Delaware Information Security Policy