**Synopsis:** Guide collaboration between the public and DTI regarding reported vulnerabilities.

**Authority:** Title 29, Delaware Code, §9004C - General powers, duties and functions of DTI "2) Implement statewide and interagency technology solutions, policies, standards and guidelines as recommended by the Technology Investment Council on an ongoing basis and the CIO, including, but not limited to, statewide technology and information architectures, statewide information technology plans, development life cycle methodologies, transport facilities, communications protocols, data and information sharing considerations, the technique of obtaining grants involving the State’s informational resources and the overall coordination of information technology efforts undertaken by and between the various State agencies;”

**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:** Elayne Starkey, Chief Security Officer

**Approval By:** James Collins, Chief Information Officer

**Approved On:** 6/26/2018

**Review Date:** 6/26/2018
TABLE OF CONTENTS

Section                                                                 Page

I.  Policy                                                              2
II. Definitions                                                         5
III. Development and Revision History                                   7
IV. Approval Signature Block                                            7
V. Related Policies and Standards                                      7

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)
Delivering Technology that Innovates

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:
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.
Delivering Technology that Innovates

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
5. Related Policies and Standards
‘Delaware Information Security Policy”