gta GEORGIA TECHNOLOGY AUTHORITY	**Georgia Technology Authority**

Title:	**Vulnerability Disclosure Program (VDP) Policy**	
PSG Number:	PS-21-001	
Issue Date:	6/1/2021	**Effective Date: 6/1/2021**
Synopsis:	Establishes VDP program for the Executive Branch	

PURPOSE

The primary focus of the Vulnerability Disclosure Program (VDP) is to securely accept, triage and rapidly remediate vulnerabilities submitted by our security research community.

SCOPE and AUTHORITY

Scope

- Executive Branch State Agencies
- Any other State entities wanting to opt-in into the program.

Authority

- Information Technology Policies, Standards and Guidelines (PM-04-001)

Enterprise Information Security Charter (PS-08-005)

POLICY

The VDP program will consist of the following elements:

1. Promise: A clear, good faith commitment to participants and entities potentially impacted by security vulnerabilities.

2. Scope: Tools, assets and vulnerability types covered.

3. "Safe Harbor": Assure that the finder reporting in good faith will not be unduly penalized.

State entities will operate in good faith with researchers that submit reports through the vulnerability disclosure program. Researchers must otherwise comply

with all applicable Federal, State, and local laws in connection with security research activities. Researchers may not engage in any security research or vulnerability disclosure activity that is inconsistent with terms and conditions of the Memorandum of Understanding or the law. All participants will be registered with the Office of Information Security's approved vendor and have an approved, signed copy of the associated Memorandum of Understanding on file. The Office of Information Security reserves the right to remove a participant from the researcher pool at any time.

4. Process: The process researchers use to report vulnerabilities.

5. Preferences: A living document that sets expectations for preferences and priorities regarding how reports will be evaluated.

Collaborative Research Partnerships

Below are four groups and/or organizations who have agreed to work together in a joint endeavor to promote the broader goal of vulnerability disclosure:

- **The Cybersecurity Board**: Provide oversight and support for the program.
- **The Georgia Technology Authority**: Review and approve any associated policy pursuant to their statutory authority for IT Policy, Standards, and Guidelines for Executive Agencies.
- **The Georgia Cyber Center and Augusta University**: Leverage its academic and commercial partnerships for the execution of program and provide timely and relevant feedback on policy and standards development.
- **The Office of Information Security (OIS)**: Facilitate policy adoption through the GTA Board as appropriate and manage the overall program for the Cybersecurity Board. OIS retains responsibility for tracking identified vulnerabilities through this program. OIS will ensure agencies adequately document risk registers and provide mitigating actions in a timely manner.

TERMS AND DEFINITIONS

Researchers - Approved cybersecurity research practitioners with proven knowledge, skills, and abilities in passive penetration testing for federal and state

government.

RELATED ENTERPRISE POLICIES, STANDARDS AND GUIDELINES

N/A