	Georgia Technology Authority	
Title:	**Digital Security**	
PSG Number:	**SS-19-002**	
Effective Date:		**Review Date: 12/01/2024**
Synopsis:	Establish common set of security protocols	

PURPOSE

To establish a common set of security protocols across all State digital properties to ensure the protection of sensitive information.

SCOPE and AUTHORITY

O.C.G.A 50-25-4(a)(8) – *State Government, Georgia Technology, General Powers*
O.C.G.A 50-25-4(a)(20) - *State Government, Georgia Technology, General Powers*
PM-04-001 – *Information Technology Policies, Standards and Guidelines*
PS-08-005 – *Enterprise Information Security Policy*

STANDARD

HTTPS Requirements

All websites and web applications should deliver information via HTTPS protocol. HTTPS encrypts sensitive user information and prevents intruders from gaining access to that data or tampering with the session, such as by injecting malware or advertisements. By deprecating all use of HTTP for HTTPS, we establish trust with our users who expect that their interactions with the government be private and secure.
In addition to protecting users and safeguarding our sites from malicious attacks, adopting HTTPS-only browsing ensures that our sites are compliant with modern web standards. As more and more organizations and web consortiums adopt HTTPS, including common web APIs and search engines, we will need to ensure that our sites conform for both interoperability and optimization.

Regular Software Maintenance

All open-source software applications, websites, and services must be monitored for security-related issues and patched as quickly as possible (within 30 days of a patch release) and in a manner consistent with

change management procedures. All third-party software solutions shall be stable, maintained, and well-supported.
Solutions that have reached end-of-life, have been deprecated, or are otherwise no longer maintained by the open source community shall be replaced within 60 days of end-of-life by products that are current and receive regular security updates.

Regular Security Audit
An external, independent security audit of all websites and web applications shall be performed at a minimum of **every two years**. Systems that process and/or store more sensitive information such as personally identifiable information (PII), should be reviewed more frequently and thoroughly. Audits shall identify potential security vulnerabilities, efforts needed to remediate outstanding issues, and a timeline for implementation.

A software maintenance plan that accounts for regular security scanning and remediation is a necessary component of all web sites and applications. If you're using a content management system, such as Drupal or Wordpress, you shall only use stable modules or plugins and update all system components according to the latest security releases.

Backups
All websites and applications must be backed up to a secure location that is independent from the production environment. Backups shall contain all code, databases, and files. Backups shall be performed on a regular basis, ranging from daily to a frequency determined by potential impact to business operations.

User Account Audits
User accounts shall reflect the actual users of the system, and shall be reviewed regularly to ensure that former employees, contractors and/or vendors that are no longer employed or contracted by the State are prevented from accessing state digital properties.