Georgia Department of Public Safety
Policy Manual

SUBJECT **INFORMATION SECURITY**	POLICY NUMBER **26.01**
DISTRIBUTION **ALL EMPLOYEES**	REVISED DATE **8/9/2023**
	POLICY REVIEWED **8/9/2023**

26.01.1 Purpose

To define the mandatory minimum information security requirements for the Georgia Department of Public Safety (DPS). This policy acts as an umbrella document to all other security policies and associated standards. This policy defines the responsibility to:

A. Protect and maintain the confidentiality, integrity and availability of information and related infrastructure assets;

B. Manage the risk of security exposure or compromise;

C. Assure a secure and stable information technology (IT) environment;

D. Identify and respond to events involving information asset misuse, loss or unauthorized disclosure;

E. Monitor systems for anomalies that might indicate compromise; and

F. Promote and increase the awareness of information security.

Failure to secure and protect the confidentiality, integrity and availability of information assets in today's highly networked environment can damage or shut down systems that operate critical infrastructure, financial and business transactions, and vital government functions; compromise data; and result in legal and regulatory non-compliance.

This policy defines a framework that will assure appropriate measures are in place to protect the confidentiality, integrity, and availability of data; and assure staff and all other affiliates understand their role and responsibilities, have adequate knowledge of security policy, procedures, and practices; and finally, know how to protect information.

26.01.2 Policy

This policy encompasses all systems, automated and manual, for which DPS has administrative responsibility. This includes systems managed or hosted by third parties on behalf of the agency. It addresses all information, regardless of the form or format, which is created or used in support of business activities.

26.01.3 Definitions

A. Chief Information Officer (CIO) – The most senior member in an organization responsible for the information technology and computer systems that support enterprise goals. He/She

holds ultimate responsibility for the technology assets and security of information assets held by the agency.

B. Compliance – Ensuring that a standard or set of guidelines is followed.

C. Device – Laptop, desktop, mobile data terminal (MDT), cellular device, or any form of technology used to access Department information technology services.

D. Information Security – The concepts, techniques, technical measures, and administrative measures used to protect information assets from deliberate or inadvertent unauthorized acquisition, damage, disclosure, manipulation, modification, loss, or use.

E. Information Security Officer (ISO) – The Information security officer is responsible for planning, directing, and coordinating DPS information security policies, setting procedures, as well as guidelines, to ensure that all information systems are functional, secure, and safeguarded throughout the agency, and are in compliance with privacy, customer trust and information security laws and regulations applicable to DPS.

F. Network Manager – IT senior staff member responsible for setting up and overseeing the hardware and software utilized by DPS to connect agency servers and networks, as well as supervising other network staff members to ensure proper maintenance and stability of those servers and networks.

G. Developer Manager – IT senior staff member responsible for overseeing the development of DPS software applications used to accomplish the mission of the agency. He or she also supervises other application development staff members to ensure proper development and implementation of each application.

H. Director of Information Technology – IT senior staff member responsible for overseeing all areas of DPS Information Technology, to include the network and security team, the development team, and the IT support team.

I. Information System – The organized collection, processing, transmission, and dissemination of information in accordance with defined procedures, whether automated or manual. Information systems include non-financial, financial, and mixed systems.

J. System – A discrete set of information resources (workstations, servers, minor applications, network, etc.) working together for the collection, processing, maintenance, use sharing, dissemination, or disposition of information.

K. User – A person who uses an information technology service, application, or software.

26.01.4 Information Statement

A. Organizational Security

1. Information security requires both an information risk management function and an information technology security function. It is recommended that these functions be approved by the Commissioner or their designee.

2. DPS shall designate the IT Risk Management Team. The team shall be comprised of the following personnel:

a. CIO;

b. Director of Technology;

c. ISO;

d. Network Manager;

e. Development Director;

f. Help Desk Manager; and

g. Director of Communications.

3. The IT Risk Management Team shall be responsible for the Department's risk management function assuring that:

   a. Risk-related considerations for information assets and individual information systems, including authorization decisions, are viewed as an enterprise regarding the overall strategic goals and objectives of carrying out its core missions and business functions; and

   b. The management of information assets and information system-related security risks is consistent, reflects the risk tolerance, and is considered along with other types of risks, to ensure mission/business success.

4. DPS must designate the Cyber Security Task Force. The Task Force shall be comprised of the following personnel:

   a. CIO;

   b. Director of Technology;

   c. ISO;

   d. Network Manager;

   e. Development Director;

   f. Help Desk Manager;

   g. Director of Communications; and

   h. Network and Security Analysts.

5. Cyber Security Task Force shall be responsible for the technical information security function. For purposes of clarity and readability, this policy will refer to individual, or group, designated as the ISO or their designee. The Task Force will be responsible for evaluating and advising on information security risks.

6. Information security risk decisions must be made through consultation with the IT Risk Management Team.

7. Although the technical information security function may be outsourced to third parties, DPS retains overall responsibility for the security of the information that it owns.

B. Functional Responsibilities

1. Command Staff in conjunction with IT management are responsible for:

a. Evaluating and accepting risk on behalf of DPS;

b. Participating in the response to security incidents;

c. Complying with notification requirements in the event of a breach of private information;

d. Adhering to specific legal and regulatory requirements related to information security;

e. Communicating legal and regulatory requirements to the ISO/designated security representative; and

f. Communicating requirements of this policy and the associated standards, including the consequences of non-compliance, to users of DPS information systems and third parties, and addressing adherence in third party agreements.

2. The Cyber Security Task Force Group is responsible for:

a. Identifying information security responsibilities and goals and integrating them into relevant processes;

b. Supporting the consistent implementation of information security policies and standards;

c. Supporting security through clear direction and demonstrated commitment of appropriate resources;

d. Promoting awareness of information security best practices through the regular dissemination of materials provided by the ISO or their designee;

e. Implementing the process for determining information classification and categorization, based on industry recommended practices, organization directives, and legal and regulatory requirements, to determine the appropriate levels of protection for that information;

f. Implementing the process for information asset identification, handling, use, transmission, and disposal based on information classification and categorization; and

g. Determining who will be assigned and serve as information owners while maintaining ultimate responsibility for the confidentiality, integrity, and availability of the data.

3. The ISO is responsible for:

a. Maintaining familiarity with business functions and requirements;

b. Maintaining an adequate level of current knowledge and proficiency in information security through annual Continuing Professional Education (CPE) credits directly related to information security;

c. Assessing compliance with information security policies and legal and regulatory information security requirements;

d. Evaluating and understanding information security risks and how to appropriately manage those risks;

e. Overseeing and assuring security architecture considerations are addressed;

f. Advising on security issues related to procurement of products and services;

g. Escalating security concerns that are not being adequately addressed according to the applicable reporting and escalation procedures;

h. Disseminating threat information to appropriate parties;

i. Participating in the response to potential security incidents;

j. Participating in the development of enterprise policies and standards that considers DPS's needs; and

k. Promoting information security awareness.

4. IT Management is responsible for:

a. Supporting security by providing clear direction and consideration of security controls in the data processing infrastructure and computing network(s) which support the information owners;

b. Providing resources needed to maintain a level of information security control consistent with this policy;

c. Identifying and implementing all processes, policies, and controls relative to security requirements defined by the business and this policy;

d. Implementing the proper controls for information owned based on the classification designations;

e. Providing training to appropriate technical staff on secure operations (e.g. secure coding, secure configuration);

f. Fostering the participation of information security and technical staff in protecting information assets, and in identifying, selecting and implementing appropriate and cost-effective security controls and procedures; and

g. Implementing business continuity and disaster recovery plans.

5. Users of DPS information systems are responsible for:

a. Understanding the baseline information security controls necessary to protect the confidentiality, integrity, and availability of information entrusted;

b. Protecting information and resources from unauthorized use or disclosure;

c. Protecting personal, private, sensitive information from unauthorized use or disclosure;

d. Abiding by the Utilization of Technology policy, and all other related DPS policies; and

e. Reporting suspected information security incidents or weaknesses to the appropriate manager and ISO/designated security representative.

C. Separation of Duties

1. To reduce the risk of accidental or deliberate system misuse, separation of duties and areas of responsibility must be implemented where appropriate.

2. Whenever separation of duties is not technically feasible, other compensatory controls must be implemented. Controls such as monitoring of activities, audit trails and management supervision, and the audit and approval of security controls must always remain independent and segregated from the implementation of security.

D. Information Risk Management

1. Any system or process that supports business functions must be appropriately managed for information risk and undergo information risk assessments, at a minimum annually, as part of a secure system development life cycle.

2. Information security risk assessments are required for new projects, implementations of new technologies, significant changes to the operating environment, or in response to the discovery of a significant vulnerability.

3. DPS Command Staff, in conjunction with IT management, is responsible for selecting the risk assessment approach that will be used based on needs and any applicable laws, regulations, and policies.

4. Risk assessment results, and the decisions made based on these results, must be documented.

E. Information Classification and Handling

1. All information, which is created, acquired, or used in support of business activities, must only be used for its intended business purpose.

2. All information assets shall have an information owner established within the lines of business.

3. Information must be properly managed from its creation, through authorized use, to proper disposal.

4. Information must be classified on an ongoing basis based on its confidentiality, integrity, and availability characteristics.

5. An information asset must be classified based on the highest level necessitated by its individual data elements.

6. If DPS is unable to determine the confidentiality classification of information, or the information is personal identifying information (PII), the information must have a high confidentiality classification and, therefore, is subject to high confidentiality controls.

7. Merging of information which creates a new information asset or situations that create the potential for merging (e.g. backup tape with multiple files) must be evaluated to determine if a new classification of the merged data is warranted.

8. All reproductions of information in its entirety must carry the same confidentiality classification as the original. Partial reproductions need to be evaluated to determine if a new classification is warranted.

9. Each classification has an approved set of baseline controls designed to protect these classifications and these controls must be followed.

10. DPS must communicate the requirements for secure handling of information to its workforce.

11. A written or electronic inventory of all information assets must be maintained.

12. Content made available to the general public must be reviewed according to a process that will be defined and approved by DPS. The process must include the review and approval of updates to publicly available content and must consider the type and classification of information posted.

13. PII must not be made available without appropriate safeguards approved by DPS.

14. For non-public information, which by definition is information/data that has not been previously disclosed to the general public and is otherwise not available to the general public, to be released outside DPS, or shared between other agencies, a process must be established that, at a minimum:

    a. Evaluates and documents the sensitivity of the information to be released or shared;

    b. Identifies the responsibilities of each party for protecting the information;

    c. Defines the minimum controls required to transmit and use the information;

    d. Records the measures that each party has in place to protect the information;

    e. Defines a method for compliance measurement;

    f. Provides a signoff procedure for each party to accept responsibilities; and

    g. Establishes a schedule and procedure for reviewing the controls.

F. IT Asset Management

1. All IT hardware and software assets must be assigned to a designated business unit or individual.

2. DPS is required to maintain an inventory of hardware and software assets, including all system components (e.g. network address, machine name, software version) at a level of granularity deemed necessary for tracking and reporting. This inventory must be automated where technically feasible.

3. Processes, including regular scanning, must be implemented to identify unauthorized hardware and/or software and notify appropriate staff when discovered.

G. Personal Security

1. Users of DPS information systems must receive general security awareness training, to include recognizing and reporting insider threats, within 30 days of hire. Additional training on specific security procedures, if required, must be completed before access is provided to specific DPS sensitive information not covered in the general security training. All security training must be reinforced at least semi-annually or as directed by the State Cyber Security Board, and it must be tracked by the DPS Information Security Officer or a designee thereof.

2. All users of DPS information systems are required to abide by policy #14.01 - Utilization of Technologies, and all other related policies, and an auditable process must be in place for users to acknowledge that they agree to abide by the policy's requirements.

3. All job positions must be evaluated by the Chief Information Officer to determine whether they require access to sensitive information and/or sensitive information technology assets.

4. For those job positions requiring access to sensitive information and sensitive information technology assets, DPS Chief Information Officer, Information Security Officer and the Director of Technology must conduct workforce suitability determinations, unless prohibited from doing so by law, regulations, or contract. Depending on the risk level, suitability determinations may include, as appropriate and permissible, evaluation of criminal history record information or other reports from federal, state and private sources that maintain public and non-public records. The suitability determination must provide reasonable grounds for DPS to conclude that an individual will likely be able to perform the required duties and responsibilities of the subject position without undue risk to DPS.

5. A process must be established to repeat or review suitability determinations periodically and upon change of job duties or position.

6. DPS Technology is responsible for ensuring all issued information systems and property are returned prior to an employee's separation, and accounts are disabled, and access removed immediately upon separation.

H. Cyber Incident Management

1. DPS must have an incident response plan, with consistent standards, to effectively respond to security incidents.

2. All observed or suspected information security incidents or weaknesses are to be reported to appropriate management and the ISO/designated security representative, as quickly as possible. If a User of DPS information systems feels that cyber security concerns are not being appropriately addressed, they may confidentially contact GTA Office of Information Security directly.

3. The GTA Office of Information Security must be notified of any cyber incident which may have a significant or severe impact on operations or security, or which involves digital forensics, to follow proper incident response procedures and guarantee coordination and oversight.

I. Physical and Environmental Security

1. Information processing and storage facilities must have a defined security perimeter and appropriate security barriers and access controls.

2. A periodic risk assessment must be performed, at least annually, for information processing and storage facilities to determine whether existing controls are operating correctly and if additional physical security measures are necessary. These measures must be implemented to mitigate the risks.

3. Information technology equipment must be physically protected from security threats and environmental hazards. Special controls may also be necessary to protect supporting infrastructure and facilities, such as electrical supply and cabling infrastructure.

4. All information technology equipment and information media must be secured to prevent compromise of confidentiality, integrity, or availability in accordance with the classification of information contained therein.

5. Visitors to information processing and storage facilities, including maintenance personnel, must always be escorted.

J. Account Management and Access Control

1. All accounts must have an individual employee, or group, assigned to be responsible for account management. This may be a combination of the business unit and the Technology Section.

2. Except as described in the Account Management/Access Control Standard, access to systems must be provided through the use of individually assigned unique identifiers, known as user-IDs.

3. Associated with each user-ID is an authentication token, generally a password, which must be used to authenticate the identity of the person or system requesting access.

4. Automated techniques and controls should be implemented to lock a session and require authentication or re-authentication after a period of inactivity for any system where authentication is required. Information on the screen must be replaced with publicly viewable information (e.g. screen saver, blank screen, clock) during the session lock.

5. Automated techniques and controls should be implemented to terminate a session after specific conditions are met as defined in the Account Management/Access Control Standard.

6. Passwords used to authenticate a person or process must be treated as confidential and protected appropriately.

7. Passwords must not be stored on paper, or in an electronic file, hand-held device, or browser, unless they can be stored securely and the method of storing (e.g. password vault) has been approved by the ISO/designated security representative.

8. Information owners are responsible for determining who should have access to protected resources within their jurisdiction, and what those access privileges should be (read, update, etc.).

9. Access privileges will be granted in accordance with the user's job responsibilities and will be limited only to those necessary to accomplish assigned tasks in accordance with DPS missions and business functions (I.E. least privilege).

10. Users of privileged accounts must use a separate, non-privileged account when performing normal business transactions (e.g. accessing the Internet, e-mail).

11. Logon banners must be implemented on all systems where that feature exists to inform all users that the system is for business or other approved use consistent with policy, and that user activities may be monitored, and the user should have no expectation of privacy.

12. Advance approval for any remote access connection must be provided by the DPS Technology Section, in consultation with the ISO. An assessment must be performed and documented to determine the scope and method of access, the technical and

business risks involved and the contractual, process, and technical controls required for such connection to take place.

13. All remote connections must be made through managed points-of-entry reviewed by the ISO.

14. Working from a remote location must be authorized by management, and practices which assure the appropriate protection of data in remote environments must be shared with the individual, prior to the individual being granted remote access.

K. Systems Security

1. Systems include but are not limited to servers, platforms, networks, communications, databases, and software applications.

2. An individual or group must be assigned responsibility for maintenance and administration of any system deployed on behalf of DPS. A list of assigned individuals or groups must be centrally maintained.

3. Security must be considered at system inception and documented as part of the decision to create or modify a system.

4. All systems must be developed, maintained, and decommissioned in accordance with a secure system development lifecycle (SSDLC).

5. Each system must have a set of controls commensurate with the classification of any data that is stored on or passes through the system.

6. All system clocks should synchronize to a centralized reference time source set to UTC (Coordinated Universe Time) which is itself synchronized to at least three synchronized time sources.

7. Environments and test plans must be established to validate the system works as intended prior to deployment in production.

8. Separation of environments (e.g. development, test, quality assurance, production) is required, either logically or physically, including separate environmental identifications (e.g. desktop background, labels).

9. Formal change control procedures for all systems must be developed, implemented, and enforced. At a minimum, any change that may affect the production environment and/or production data must be included.

a. Databases and Software (including in-house or third party developed and commercial off the shelf (COTS):

1) All software written for or developed on systems must incorporate secure coding practices, to avoid the occurrence of common coding vulnerabilities and to be resilient to high-risk threats, before being deployed in production.

2) Once test data is developed, it must be protected and controlled for the life of the testing in accordance with the classification of the data.

3) Production data may be used for testing only if a business case is documented and approved in writing by the information owner and the following controls are applied:

a) All security measures, including but not limited to access controls, system configurations and logging requirements for the production data, are applied to the test environment and the data is deleted as soon as the testing is completed; or

b) Sensitive data is masked or overwritten with fictional information.

4) Where technically feasible, development software and tools must not be maintained on production systems.

5) Where technically feasible, source code used to generate an application or software must not be stored on the production system running that application or software.

6) Scripts must be removed from production systems, except those required for the operation and maintenance of the system.

7) Privileged access to production systems by development staff must be restricted.

8) Migration processes must be documented and implemented to govern the transfer of software from the development environment up through the production environment.

b. Network Systems:

1) Connections between systems must be authorized by the DPS Commissioner or their designee, the Commissioner of all relevant agencies and protected by the implementation of appropriate controls.

2) All connections and their configurations must be documented, and the documentation must be reviewed by the information owner and the ISO annually, at a minimum, to assure:

a) The business case for the connection is still valid and the connection is still required; and

b) The security controls in place (filters, rules, access control lists, etc.) are appropriate and functioning correctly.

3) Network architecture must be maintained that includes, at a minimum, tiered network segmentation between:

a) Internet accessible systems and internal systems;

b) Systems with high security categorizations (e.g., mission critical, systems containing PII) and other systems; and

c) User and server segments.

4) Network management should be performed from a secure, dedicated network.

5) Authentication is required for all users connecting to internal systems.

6) Network authentication is required for all devices connecting to internal networks.

7) Only authorized individuals or business units may capture or monitor network traffic.

8) A risk assessment must be performed, in consultation with the ISO, before the initiation of, or significant change to, any network technology or project, including but not limited to wireless technology.

L. Collaborative Computing Devices

1. Collaborative computing devices must:

a. Prohibit remote activation; and

b. Provide users physically present at the device with an explicit indication of use.

2. Must provide simple methods to physically disconnect collaborative computing devices.

M. Vulnerability Management

1. All systems must be scanned for vulnerabilities before being installed in production and periodically thereafter.

2. All systems are subject to periodic penetration testing.

3. Penetration tests are required periodically for all critical environments/systems.

4. Where DPS has outsourced a system to another agency or a third party, vulnerability scanning/penetration testing shall be conducted.

5. Scanning/testing and mitigation must be included in third party agreements.

6. The output of the scans/penetration tests will be reviewed in a timely manner by the system owner. Copies of the scan report/penetration test must be shared with the ISO for evaluation of risk.

7. Appropriate action, such as patching or updating the system, must be taken to address discovered vulnerabilities. For any discovered vulnerability, a plan of action and milestones must be created, and updated accordingly, to document the planned remedial actions to mitigate vulnerabilities.

8. Any vulnerability scanning/penetration testing must be conducted by individuals who are authorized by the ISO. Any other attempts to perform such vulnerability scanning/penetration testing shall be deemed an unauthorized access attempt.

9. Anyone authorized to perform vulnerability scanning/penetration testing must have a formal process defined, tested and followed at all times to minimize the possibility of disruption.

N. Operations Security

1. All systems and the physical facilities in which they are stored, must have documented operating instructions, management processes and formal incident management procedures related to information security matters which define roles and responsibilities of affected individuals who operate or use them.

2. System configurations must follow approved configuration standards.

3. Advance planning and preparation must be performed to ensure the availability of adequate capacity and resources. System capacity must be monitored on an ongoing basis.

4. Where DPS provides server, application, or network service to another agency, operational and management responsibilities must be coordinated by all impacted agencies.

5. Controls must be implemented (e.g., anti-virus, software integrity checkers, web filtering) across systems where technically feasible, to prevent and detect the introduction of malicious code or other threats.

6. Controls must be implemented to disable automatic execution of content from removable media.

7. Controls must be implemented to limit storage of information to authorized locations.

8. Controls should be in place to allow only approved software to run on a system and prevent execution of all other software.

9. All systems must be maintained at a vendor-supported level to ensure accuracy and integrity.

10. All security patches must be reviewed, evaluated, and appropriately applied in a timely manner. This process must be automated, where technically possible.

11. Systems which can no longer be supported or patched to current versions should be removed.

12. Systems and applications must be monitored and analyzed to detect deviation from the access control requirements outlined in this policy and the Security Logging Standard, and record events to provide evidence and to reconstruct lost or damaged data.

13. Audit logs recording exceptions and other security-relevant events must be produced, protected, and kept consistent with record retention schedules and requirements.

14. Monitoring systems should be deployed (e.g., intrusion detection/prevention systems) at strategic locations to monitor inbound, outbound, and internal network traffic.

15. Monitoring systems should be configured to alert incident response personnel to indications of compromise or potential compromise.

16. Contingency plans (e.g., business continuity plans, disaster recovery plans, continuity of operations plans) must be established and tested at least annually, to obtain the following objectives:

    a. An evaluation of the criticality of systems used in information processing (including but not limited to software and operating systems, firewalls, switches, routers, and other communication equipment).

    b. Recovery Time Objective (RTO)/Recovery Point Objective (RPO) for all critical systems.

17. Backup copies of DPS information, software, and system images must be taken regularly in accordance with DPS's defined requirements.

18. Backups and restoration must be tested regularly. Separation of duties must be applied to these functions.

19. Procedures must be established to maintain information security during an adverse event. For those controls that cannot be maintained, compensatory controls must be in place.

O. Compliance

This policy shall take effect upon publication. Compliance is expected with all enterprise policies and standards. Policies and standards may be amended at any time; compliance with amended policies and standards is expected.

If compliance with this standard is not feasible or technically possible, or if deviation from this policy is necessary to support a business function, DPS shall request an exception through Georgia's Chief Information Security Officer's exception process.

P. Revision History

This standard shall be subject to periodic review to ensure relevancy.

Example of periodic review maintained by the ISO.

Date	Description of Change	Reviewer
04/04/2022	Original Policy	Jeremy King
08/22/2022	Draft	Capt. Bryant, Brentwood, Romyr, Jeremy, Holly, Vanishree, Monnie, Eric
02/24/2022	Draft	Capt. Bryant, Brentwood, Holly Smith