NJ OFFICE OF INFORMATION TECHNOLOGY
Chris Christie, Governor
E. Steven Emanuel, Chief Information Officer

P.O. Box 212   www.nj.gov/it/ps/
300 Riverview Plaza
Trenton, NJ 08625-0212

STATE OF NEW JERSEY IT CIRCULAR **Title:** 130-01 – Information Assets Classification and Control Standard	**NO:** 08-04-S1-NJOIT	**SUPERSEDES:** N/A
	DATE PUBLISHED: June 6, 2012	
	VERSION: 1.0	**EFFECTIVE DATE:** Date of Signature
	FOR INFORMATION CONTACT: Office of Policy and Planning oitpolicy@oit.state.nj.us	

ATTN: Directors of Administration and Agency IT Leaders

I. PURPOSE

This standard establishes security classification categories for both information and information systems. This standard supports the Executive Branch of New Jersey State Government's ability to accomplish its assigned mission, protect its assets, fulfill its legal responsibilities, maintain its day-to-day functions and protect individual's information.

Note: Any Federal or State legislation, regulations or mandates to classify data in a manner that requires tighter controls than articulated in this standard shall take precedence.

The procedures for maintaining inventories of asset classification will be deferred to *08-04-P1-NJOIT, Information Assets Classification and Control Procedures*.

II. AUTHORITY

This standard is established under the authority of *08-04-NJOIT, Information Assets Classification and Control Policy*.

Office of Information Technology (OIT) reserves the right to change or amend this circular to comply with changes in State standards.

III. SCOPE

This standard applies directly to all personnel including employees, temporary workers, volunteers, contractors and those employed by contracting entities, those who develop and administer information systems and resources and others tasked to implement *08-04-NJOIT, Information Assets Classification and Control Policy*.

IV. DEFINITIONS

Please refer to the Statewide Policy Glossary at http://www.nj.gov/it/ps/glossary/.

V. STANDARD

Security classification categories are to be used in conjunction with vulnerability and threat information when assessing the risk to an organization, and for fiscal and strategic planning. Information assets shall be classified by the Data Steward and entered into OIT's Application/Server Asset Inventory (ASAI) database.

A. Asset Sensitivity

Sensitivity classification identifies information in terms of what it is and how access, processing, communications and storage must be controlled. Information assets shall be classified in terms of sensitivity. All information stored, processed or transmitted by information resources shall be identified by one of four levels of sensitivity: Public, Secure, Confidential and Personal. If more than one sensitivity level could apply to the information, the highest level (most restrictive) will be selected.

1. **Public** – Information that is authorized for release to the public. The disclosure, unauthorized access, or unauthorized use of Public information would not adversely impact OIT, the state, and/or the public. Examples include: List of New Jersey municipalities and cabinet officials.

2. **Secure** – Information that is available to business units and used for official purposes but would not be released to the public unless requested. The disclosure, unauthorized access, or unauthorized use of secure information would have a limited adverse impact on OIT, the state, and/or the public. Examples include: Financial accounting information and department projects such as Department of Transportation bridge maintenance records.

3. **Confidential** – Information of a sensitive nature that is available only to designated personnel. The disclosure, unauthorized access, or unauthorized use of confidential information would have a significant adverse impact on OIT, the State and/or the public. Confidential information would be undiscoverable under the Open Public Records Act (OPRA). Examples include: Criminal investigation for fraud and Homeland Security planning and support.

4. **Personal** – All personally identifiable information (PII) pertaining to individuals that is protected by Federal or State law shall be labeled as Personal. The disclosure, unauthorized access, or unauthorized use of Personal information would have a significant adverse effect on OIT, the

State and/or the public and the individuals whose information was disclosed. Examples include: Personal financial information, Social Security number and medical conditions.

> Note: Sensitivity classifications shall attach to and follow the information to which it applies until the classification is changed by the Data Steward.

B. Electronic Authentication

Electronic authentication is a process of establishing confidence and assurance in the user identity when granting access to an information asset. Electronic authentication presents technical challenges to the user based on secrets.

Levels of assurance are determined based on a risk assessment of the electronic authentication and the information asset. The assessment identifies the risks and their likelihood of occurrence. Agencies must determine the required level of assurance for the information asset's authentication and transaction.

Level 1 is the lowest assurance and Level 4 is the highest.

1. **Level 1** – No identity proofing required. A simple password challenge-response can be presented before granting access.

2. **Level 2** – Provides single factor authentication and identity proofing is required. A user id and password is presented before granting access. A password policy is enforced based on the sensitivity of the information asset.

3. **Level 3** – Provides multi-factor authentication, and two forms of identity proofing are required. The two forms are a physical or software token in combination with a user id and password. The user must unlock the token with a credential.

4. **Level 4** – Provides multi-factor authentication, and two forms of identity proofing are required. The two forms are a physical token in combination with a user id and password. Level 4 token requirements can be met by using the card authentication key of a FIPS 201 compliant Personal Identity Verification (PIV) card.

C. Asset Criticality

Criticality classifies the importance of specific information to operations in terms of the impact that loss of use of the information would have on the organization. Criticality ranks the significance of the information to the organization's mission.

Most often, the criticality value assists in determining recovery priorities during a disaster with the most critical systems being recovered first.

Information shall be classified by one of four criticality levels: Derived, Non-Essential, Essential or Public Safety.

1. **Derived** – Information/data that is derived from other systems and is dependent upon that system and the restoration of that data. The loss of Derived data and/or its processing platforms would be minor and would not impact operations. Examples include: Data warehousing (data downstream from source) and internal reporting databases created to supply reports.

2. **Non-Essential** – Data that is not mission essential to the business unit and can be restored after all essential data is made available. The loss of Non-Essential data and/or its processing platforms would have a minimal impact on operations. The acceptable loss of Non-Essential information would typically be expressed in days. Examples include: Correspondence tracking systems and project management data.

3. **Essential** – Data that is essential to the mission of the business unit and must be restored as quickly as possible. The loss of Essential data and/or its processing platforms would adversely effect operations. The acceptable loss of Essential information would typically be expressed in hours. Examples include: Motor vehicle licensing and benefit checks.

4. **Public Safety** – Data to support life and property safety, which must be available at all times. The loss of Public Safety data and/or its processing platforms could be catastrophic to operations. Public Safety information is typically redundant and these types of systems are the first to be recovered during a disaster. The acceptable loss of Public Safety information or an information resource that processes this data would typically be expressed in minutes. Examples include: State Criminal Information Center (SCIC) data and critical infrastructure data (e.g., telecommunications, utilities, 911).

> Note: If more than one criticality level could apply to the information when aggregated, the highest level (most critical) will be selected.

a) Information assets shall be classified in terms of low, moderate, or high impact of loss on each of the following: availability, integrity, and confidentiality of the assets with the higher the impact the greater the security control required. The loss classification should have some correlation to both the sensitivity and criticality levels.

1. **Low Impact** –Loss of availability, integrity and confidentiality could have a limited adverse effect on organizational operations, organizational assets or individuals. Public information is often categorized as having a low impact.

2. **Moderate Impact** –Loss of availability, integrity and confidentiality could have a serious adverse effect on organizational operations, organizational assets or individuals. Secure data would be categorized as having a limited impact.

3. **High Impact** – Loss of availability, integrity and confidentiality could have a severe and/or catastrophic adverse effect on organizational operations, organizational assets and/or individuals. Confidential and/or personal information should be categorized as having a high impact.

D. Physical assets shall inherit the highest criticality value of the information they process, store and/or communicate. Physical assets must not contribute to the degradation of the classification of the information. Wherever and whenever practicable, information assets shall be segregated according to like classification.

E. Classifications shall be used for security control decisions, risk management, fiscal and strategic planning as well as to aid in application and system development and implementation.

Sensitivity and impact values shall be used to establish data protection requirements. (e.g., information classified as Confidential would require more security controls than information classified as Public.) Only those security controls that fulfill the defined protection requirements and are acknowledged as providing an acceptable level of risk will be implemented.

Criticality values shall be used to ensure that platform/application specifications and implemented controls are sufficient to meet the availability requirements of the asset.

Classification values (potential loss impact, sensitivity and criticality) shall be an input to:

1. Authentication and authorization decision makers to ensure appropriate access control is established and maintained for all users and systems are provisioned and deprovisioned in an accountable fashion.

2. Developers, in support of the New Jersey Data Management Framework and Common Data Architecture.

3. Disaster Recovery/Business Continuity planners to ensure recovery priorities are appropriate.

4. Fiscal Planning to provide decision making input support of the yearly Appropriations act as it relates to IT purchasing.

5. Strategic Planning and Development.

VI. RESPONSIBILITIES

All responsibilities shall be delegated as stated in *08-04-NJOIT, Information Assets Classification and Control Policy*.

VII. EXCEPTIONS AND NON-COMPLIANCE

Departments and Agencies shall comply with this standard within 90 days of its effective date.

Failure to comply with this standard may result in disciplinary action. A compliance exception must be requested if there is an inability to comply with this standard because of a business reason or system constraint. Exceptions and noncompliance with this standard shall be managed in accordance with *08-02-NJOIT, Information Security Managing Exceptions Policy.*

Signature on File   *6/15/2012*

E. STEVEN EMANUEL   **DATE**
Chief Technology Officer-NJ Office of Information Technology
State Chief Information Officer