NJ OFFICE OF INFORMATION TECHNOLOGY
Philip D. Murphy, Governor
Odysseus Marcopolus, Chief Operating Officer

P.O. Box 212
300 Riverview Plaza
Trenton, NJ 08625-0212

www.tech.nj.gov

STATE OF NEW JERSEY TECHNOLOGY CIRCULAR 130-01 – Information Assets Classification and Control Standard	**POLICY NO:** 08-04-S1-NJOIT	
	SUPERSEDES: NEW	**EFFECTIVE DATE:** 06/15/2017
	VERSION: 2.0	**LAST REVIEWED:** 09/02/2015

ATTN: Directors of Administration and Agency IT Managers

1 PURPOSE

This standard establishes security classification categories for both information and information systems. This standard supports the New Jersey State Government's ability to protect its assets, fulfill its legal responsibilities, maintain its day-to-day functions, and protect individuals' 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, *130-00-01 – Information Assets Classification and Control Procedure.*

2 AUTHORITY

This standard is established under the authority of 08-04-NJOIT, *130 – Information Asset Classification Control Policy.*

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

3 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, *130 - Information Assets Classification Control Policy.*

4 DEFINITIONS

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

5 STANDARD

Security classification categories are to be used in conjunction with vulnerability and threat information in assessing the risk to an organization, as well as for fiscal and strategic planning. Information assets shall be classified by the Department/Agency and entered into OIT's Statewide Office of Information Security Asset Classification System.

Asset Classifications shall be used for making decisions about security controls risk management, fiscal issues, and strategic planning as well as to aid in application and system development and implementation.

Data protection requirements will be based on the sensitivity of the data and its importance to State operations (e.g. sensitivity and impact values.). Security controls must fulfill the defined protection requirements and provide an acceptable level of risk.

Classification values shall be used as part of strategy for:

5.1.1 Assessment of the risk to an organization, and used in conjunction with vulnerability and threat information.

5.1.2 Maintenance of appropriate access control (authentication and authorization). The goal is to ensure controls are established and maintained for all users and systems are provisioned and de-provisioned in an accountable fashion.

5.1.3 Disaster Recovery/Business Continuity planning to ensure recovery priorities are appropriate.

5.1.4 Fiscal planning to provide decision making input support of the yearly appropriations act as it relates to IT purchasing.

5.1.5 Strategic Planning and Development.

5.1.5.1 ***Asset Sensitivity*** *-- Sensitivity classification categorizes information based on what it is and how its 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 categorized by one of three levels of sensitivity: Public, Secure and Sensitive. If more than one sensitivity level could apply to the information, the highest level (most restrictive) will be selected.*

5.1.5.2 ***Public*** *– Information that is authorized for release to the public. Examples include: List of New Jersey municipalities and Cabinet officials.*

5.1.5.3 ***Secure*** *– Information that is available to business units, and used for official purposes but would not be released to the public unless requested and legally reviewed. This information will be restricted to certain employees of the State of New Jersey who have a legitimate purpose for accessing this information. Examples include: asset management information and department projects such as Department of Transportation bridge maintenance records.*

5.1.5.4 ***Sensitive*** *– Information that is available only to designated personnel and would not be released to the public. Among the protected categories are information related to:*

5.1.5.4.1 Criminal Investigation

5.1.5.4.2 Homeland Security

5.1.5.4.3 Federal Employer Identification Numbers (FEINs)

5.1.5.4.4 Personal Financial

5.1.5.4.5 Personal Medical

5.1.5.4.6 Personal Identifiable

5.1.5.4.7 Social Security numbers

5.1.5.4.8 Business

5.1.5.4.9 Other

5.1.5.5 Potential Loss Impact

Information assets shall be classified (Low, Moderate, High) relative to the impact a loss would have on each of the following asset security objectives: Confidentiality, Availability, and Integrity. The higher the impact, the greater the security control required.

Security Objective	LOW	MODERATE	HIGH
Confidentiality Preserving authorized	The unauthorized disclosure of information could	The unauthorized disclosure of information could	The unauthorized disclosure of information could

restrictions on **information access and disclosure**, including means for protecting personal privacy and proprietary information. [44 U.S.C., SEC. 3542]	be expected to have **a limited adverse effect** on organizational operations, organizational assets, or individuals.	be expected to have **a serious adverse effect** on organizational operations, organizational assets, or individuals.	be expected to have **a severe or catastrophic adverse effect** on organizational operations, organizational assets, or individuals.
Integrity Guarding against improper information **modification or destruction**, and includes ensuring information non-repudiation and authenticity. [44 U.S.C., SEC. 3542]	The unauthorized modification or destruction of information could be expected to have **a limited adverse effect** on organizational operations, organizational assets, or individuals.	The unauthorized modification or destruction of information could be expected to have **a serious adverse effect** on organizational operations, organizational assets, or individuals.	The unauthorized modification or destruction of information could be expected to have **a severe or catastrophic adverse effect** on organizational operations, organizational assets, or individuals.
Availability Ensuring **timely and reliable access** to and use of information. [44 U.S.C., SEC. 3542]	The disruption of access to or use of information or an information system could be expected to have **a limited adverse effect** on organizational operations, organizational assets, or individuals.	The disruption of access to or use of information or an information system could be expected to have **a serious adverse effect** on organizational operations, organizational assets, or individuals	The disruption of access to or use of information or an information system could be expected to have **a severe or catastrophic adverse effect** on organizational operations, organizational assets, or individuals.

5.1.6 Access Control Platform

Information assets are accessible through multiple access control platforms. The platforms will vary based on the level of risk and type of network: 1) Internet, 2) Intranet or 3) Extranet. The type of platforms will vary but

common types include a portal, VPN, or custom (code) and communication protocols (http/https).

5.1.7 Level of Assurance

Level of Assurance is the degree of confidence in the process used to establish the identity of an individual to whom the credential was issued. It is a measure of the degree of confidence that the State has that the individual who used the credential is the same individual to whom the credential was issued in accordance with OMB M-04-04 (E-Authentication Guidance) and NIST 800-63 (Electronic Authentication Guidelines).

Level of assurance is determined based on a risk assessment of potential harm or impact, and the likelihood of such harm or impact.

Level 1 is the lowest Level of Assurance and Level 4 is the highest.

5.1.7.1 ***Level 1*** *– Little or no confidence in the asserted identity's validity. A simple password challenge-response can be presented before granting access.*

5.1.7.2 ***Level 2*** *– Some confidence in the asserted identity's validity. Identity proofing is required. A user ID and password are presented before granting access. A password policy is enforced based on the sensitivity of the information asset.*

5.1.7.3 ***Level 3*** *– High confidence in the asserted identity's validity. 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.*

5.1.7.4 ***Level 4*** *– Very high confidence in the asserted identity's validity. Two forms of identity and in person proofing are required. In person identity-proofing is required. Level 4 requires strong cryptographic authentication of all communicating parties and all sensitive data transfers between the parties.*

5.1.8 Electronic Authentication (User Credential)

5.1.8.1 ***Level 1*** *– A simple password challenge-response can be presented before granting access.*

5.1.8.2 ***Level 2*** *– A knowledge-based authentication, user ID and password, or user ID and SMS-one time password is presented before granting access. A password policy is enforced based on the sensitivity of the information asset.*

5.1.8.3 ***Level 3*** *– Multi-factor authentication and two forms of identity proofing are required. The two forms are a software or physical token in combination with a user ID and password.*

5.1.8.4 ***Level 4*** *– Authentication based on proof of possession of a key through a cryptographic protocol. At this level, in-person identity proofing is required. Level 4 requires strong cryptographic authentication of all communicating parties and all sensitive data transfers between the parties.*

5.1.9 Physical Asset Classification

Physical assets shall inherit the highest classification 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.

6 RESPONSIBILITIES

All responsibilities shall be delegated as stated in 08-04-NJOIT, *130 - Information Assets Classification Control Policy.*

7 EXCEPTIONS AND NON-COMPLIANCE

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

Requests for exceptions for non-compliance with this standard shall be managed in accordance with 08-04-NJOIT, *130 - Information Assets Classification Control Policy*.