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 – Information Asset Classification Control Policy	**POLICY NO:** 08-04-NJOIT	
	SUPERSEDES: NEW	**EFFECTIVE DATE:** 07/31/2008
	VERSION: 3.0	**LAST REVIEWED:** 09/02/2015

ATTN: Directors of Administration and Agency IT Managers

1 PURPOSE

The purpose of this policy is to provide a mechanism to ensure the proper classification of all information assets. This policy establishes the criteria for complying with federal and local regulations regarding privacy and confidentiality of information by ensuring an appropriately risk managed Information Technology infrastructure through proper classification. This policy further establishes the prioritization of confidential and personal information and/or to identify the most significant risks to the Executive Branch of New Jersey State Government's systems. The purpose is also to ensure access to information that is processed, stored, and/or transmitted across the Executive Branch of New Jersey State Government's systems is properly controlled. This policy further establishes requirements to ensure that all data, applications and systems are inventoried for security control purposes and to assist in fiscal, strategic and risk management planning requirements. The criteria for classification are identified in *130-01 – Information Assets Classification and Control Standard*, 08-04-S1-NJOIT. The process for classification is identified in *130-00-01 – Information Assets Classification and Control Procedure*, 08-04-P1-NJOIT.

2 AUTHORITY

This policy is established under the authority of the State of New Jersey. N.J.S.A. 52:18a-230 b. This policy defines New Jersey Office of Information Technology's (NJOIT) role with regard to technology within the Executive Branch community of State Government.

The New Jersey Office of Information Technology (NJOIT) reserves the right to change or amend this circular.

3 SCOPE

This policy applies directly to all personnel including employees, temporary workers, volunteers, contractors and those employed by contracting entities, and others who develop and administer information systems and resources for those systems.

The scope of this policy includes the following:

3.1 Information assets used by the New Jersey State Government for external and client operations.

3.2 Physical assets that process, store, or transmit information for the New Jersey State Government.

4 POLICY

All departments and agencies have a responsibility to protect the confidentiality, integrity, and availability of information generated, accessed, modified, transmitted, stored or used by the New Jersey State Government, irrespective of the electronic or digital medium on which the information resides and regardless of format.

Accountability for all Information Assets will be maintained through an inventory management process that will align with and support fiscal, strategic and risk management planning.

The following are information asset classification and control requirements that must be implemented across the New Jersey State Government systems.

4.1 All departments and agencies must be aware of, determine classification of, and maintain an inventory of all information assets according to the Information Asset Classification and Control standard and procedures.

4.2 All information and data assets shall be classified in terms of sensitivity and potential loss impact on departments and/or agencies should that information become unavailable.

4.3 All physical assets shall be classified in terms of potential loss impact on departments and/or agencies should that information become

unavailable. Systems will inherit a sensitivity classification based on the highest level of classification of the data that it processes or stores.

4.4 Classifications shall be used for security control decisions, including access control and authorization, risk mitigation, application development and maintenance decisions, architectural design decisions, and fiscal and strategic planning decisions.

4.5 It is the responsibility of the department or agency to classify their information assets and mark their respective media accordingly.

4.6 All department and agency physical systems used to house the information must be adequate to protect said information according to its classification.

4.7 Information assets and associated classifications shall be maintained by the Office of Information Technology's Statewide Office of Information Security in a central asset classification system.

5 DEFINITIONS

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

6 RESPONSIBILITIES

6.1 Department/Agency

6.1.1 Identify the potential loss impact and sensitivity levels of their information being processed, stored, or transmitted by information resources according to any identified prioritization schedule as defined in the procedure document.

6.1.2 Maintain timely updates and maintain a cognizance at all times of the values of the information assets within their management.

6.1.3 Be aware of and specify, as needed the functional security requirements for the information or physical assets needed to protect those assets.

6.1.4 Approve all access and restriction requirements to their information/data and maintain current access control lists for such information/data.

6.1.5 Specify procedures for the access, processing, maintenance, storage, protection, and/or destruction of information/data.

6.1.6 Review any security reports of the processing environment provided by the Statewide Office of Information Security, Department/Agency's security advisor or hosting provider to ensure an acceptable level of risk is established to guard against the loss of information/data confidentiality, integrity, or availability.

6.1.7 Provide classification inventory of their information and physical assets as required.

6.1.8 Be cognizant of all regulatory compliance requirements for data and provide information about regulatory compliance to the Statewide Office of Information Security, Department/Agency's security adviser or hosting provider.

6.1.9 Ensure all employees and business partners understand the classification values of information assets being used and are informed of procedures for protecting and releasing that information.

6.1.10 Ensure that the security controls in place are adequate to meet the asset classification requirements.

6.1.11 Administer the department or agency-defined access requirements to the information, software, and/or physical assets.

6.1.12 Ensure all employees and business entities understand the classification value of information assets being maintained or accessed and are informed of procedures for protecting and releasing that information.

6.2 Statewide Office of Information Security

6.2.1 Maintain and update the consolidated asset classification inventory.

6.2.2 Recommend security controls that satisfy the security requirements.

7 EXCEPTIONS AND NON-COMPLIANCE

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

Requests for exceptions for non-compliance with this policy shall be managed in accordance with Policy 08-02-NJOIT, *111 – Information Security Managing Exceptions.*