



<p>State of New Jersey IT Circular</p> <p>Title: 130 – Information Asset Classification Control Policy</p>	<p>POLICY: 08-04-NJOIT</p>	<p>SUPERCEDES:</p>
	<p>DATE PUBLISHED: 07-31-08</p>	
	<p>VERSION: 2.0</p>	<p>EFFECTIVE DATE: IMMEDIATELY</p>
	<p>FOR INFORMATION CONTACT: Elizabeth Caldwell, Office of Policy and Planning (609) 633-0429</p>	

ATTN: Directors of Administration and Agency IT Managers

I. 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 Information Asset Classification and Control Standard 08-04-S1-NJOIT. The process for classification is identified in Information Asset Classification and Control Procedures 08-04-S1-P1-NJOIT.

II. AUTHORITY

This policy is established under the authority of State of New Jersey P.L.2007.c.56.

OIT reserves the right to change or amend this circular to comply with changes in Agency policies.

III. 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:

- Information assets used by the Executive Branch of New Jersey State Government for external and client operations.
- Physical assets that process, store, or transmit information for the Executive Branch of New Jersey State Government.

IV. 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 Executive Branch of 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 Executive Branch of New Jersey State Government systems.

- A. All departments and agencies must be aware of, determine classification of, and maintain an inventory of all information assets of which they are either Owners or Stewards according to the Information Asset Classification and Control standard and procedures.
- B. All information and data assets shall be classified in terms of criticality, sensitivity, and potential loss impact on departments and/or agencies should that information become unavailable.
- C. All physical assets shall be classified in terms of criticality and 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.
- D. 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.
- E. It is the responsibility of the Data Steward to classify their information assets and mark their respective media accordingly.

- F. All departments and agencies physical systems used to house the information must be adequate to protect said information according to its classification.
- G. Information assets and associated classifications shall be maintained by OIT in the centralized automated Application/Server Asset Inventory application. This applies to all assets currently owned or managed by OIT. During agency consolidation, all information assets shall be incorporated into this inventory. Prior to consolidation, agencies shall maintain their own asset inventory list.

V. DEFINITIONS

A. Information Assets

Information Assets are defined as all categories of electronic devices that process and/or contain digital information including but not limited to the following: databases, records, files, electronic documents, stored data, applications, and other software that is required to support business processes such as application software and system software.

B. Physical Assets

Physical assets are defined as all computing, telecommunication and other devices that process and contain digital information including but not limited to, processors, monitors, laptops, modems, hand-held wireless devices, communications equipment (routers, switches, firewalls, etc.), magnetic media (tapes and disks), and other technical equipment.

C. Data Owner

A Data Owner is the authority, individual or organization that has legal rights to the data and those rights are protected by law. The legal rights of a Data Owner include copyright and intellectual property rights as well as the rights to exploit and/or destroy the data. The rights of the Data Owner apply even when the owned data is collected by a third party and/or combined with data owned by others.

D. Data Steward

A Data Steward is the authority, individual, or organization responsible for the use of data within his/her functional areas. The Data Steward is responsible for developing decisions specifically related to the use of the data. Data Stewards follow and/or approve policies, procedures, and guidelines that pertain to the data during the lifecycle of that data entrusted to their stewardship. Data Stewards specify procedures for the access, processing, maintenance, storage, protection, and/or destruction

of data on behalf of the Data Owner. The Data Steward may also be the Data Owner.

E. Data Custodian

A Data Custodian is the authority, individual, or organization responsible for implementing Data Steward-defined requirements while protecting the rights of the Data Owner for the access, processing, maintenance, storage, protection, and/or destruction of data and electronic records. Information/Data Custodians are responsible and accountable for the management and care of the data under their control.

VI. RESPONSIBILITIES

A. Data Stewards

1. Identify the potential loss impact, criticality, 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.
2. Maintain timely updates and maintain a cognizance at all times of the values of the information assets within their ownership and/or stewardship.
3. Be aware of and specify, as needed the functional security requirements for the information or physical assets needed to protect those assets.
4. Approve all access and restriction requirements to their information/data and maintain current access control lists for such information/data.
5. Specify procedures for the access, processing, maintenance, storage, protection, and/or destruction of information/data.
6. Review any security reports of the processing environment provided by the Data Custodian to ensure an acceptable level of risk is established to guard against the loss of information/data confidentiality, integrity, or availability.
7. Provide classification inventory of their information and physical assets to Data Custodian as required.

8. Be cognizant of all regulatory compliance requirements for data in their stewardship and provide information about regulatory compliance to data custodians.
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.

B. Data Custodian

1. Maintain and update information in the enterprise Application/Server Asset Inventory.
2. Recommend and/or implement security controls that satisfy the security requirements specified by the Data Steward.
3. Ensure that the controls in place are adequate to meet the asset classification requirements.
4. Administer the Data Steward-defined access requirements to the information, software, and/or physical assets.
5. Ensure all employees and business partners understand the classification values of information assets being maintained or accessed and are informed of procedures for protecting and releasing that information.

VII. EXCEPTIONS AND NON-COMPLIANCE

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

Failure to comply with this policy may result in disciplinary action. A compliance exception must be requested if there is an inability to comply with this policy because of a business reason or system constraint. Exceptions and non-compliance with this policy shall be managed in accordance with Policy 08-02-NJOIT (111 – *Information Security Managing Exceptions*).

Document History		
Version	Effective Date	Reason for Change
1.0	07-31-2008	Changed to a Statewide IT Circular
2.0	07-31-2008	Revised and Changed to a Statewide IT Circular

Adel W. Ebeid

Adel Ebeid, Chief Technology Officer
NJ Office of Information Technology