Cyber Command

P-RA-01

Policy – Information Classification and Management

Policy Effective Date: February 19, 2019

VERSION CONTROL

Version	Description of Change	Approver	Date
1.0	<Final Draft>	Geoff Brown	2/19/19

1 PURPOSE

The purpose of this policy is to ensure that all New York City ("NYC") Agency information is identified, classified, protected, and managed throughout its life cycles according to the information classification and management standards S-RA-01 developed by New York City Cyber Command ("NYC3"). This policy does not conflict, pre-empt, or in any way interfere with an Agency's responsibility to adhere to all applicable local, state, and federal laws, regulations, and guidelines pertaining to information privacy and security.

2 SCOPE

This policy applies to all NYC agencies, offices, departments, entities, and personnel working on behalf of or in service to New York's City's municipal government. This policy applies to all information that represents as official products or interfaces with the City of New York. This policy is consistent with NIST 800-53 security control RA 2 – (Security Categorization).

3 ROLES AND RESPONSIBILITIES

3.1 Agency head is responsible for:

3.1.1 Ensuring the correct and thorough implementation of citywide cybersecurity policies throughout the entire agency.

3.1.2 Ensuring the completeness and adequacy of all City Agency activities and documentation provided to ensure compliance with citywide cybersecurity policies throughout the entire agency.

3.1.3 Promoting efforts within the Agency to establish and maintain effective and appropriate use of Agency information.

3.1.4 Owning the data for all Agency Data sets or assigning a delegate information owner for each set of Agency Data.

3.1.5 Ensuring citywide policies are periodically reviewed and controls are put in place at the Agency to reflect changes in requirements.

3.1.6 Ensuring the Information Classification results (including supporting rationale) are documented in the agency security plan.

3.1.7 Ensuring the development and implementation of adequate controls enforcing this policy.

3.1.8 Ensuring all personnel understand their responsibilities with respect to securing agency information.

3.1.9 Auditing and logging employee activities to ensure compliance.

3.1.10 Ensuring system owners of Agency Information adhere to this policy regarding classification of information.

4 POLICY

4.1 This policy requires City Agencies and Entities to classify all information documented, processed, stored, and transmitted as:

4.1.1 Restricted Information: This is the highest level of sensitivity. Information should be classified as "Restricted Information" where the unauthorized disclosure, alteration or destruction would cause a significant level of risk to the Agency.

4.1.2 Sensitive Information: This information is only intended for internal Agency use. Information should be classified as "Sensitive Information" where the unauthorized disclosure, alteration or destruction would cause a moderate level of risk to the Agency.

4.1.3 Non-restricted Information: Public disclosure of such information is not likely to compromise individuals, operations, or the City's ability to deliver services efficiently and effectively. Information should be classified as "Non-Restricted Information" where the unauthorized disclosure, alteration or destruction of the information would have no risk to the Agency, its critical functions, its workforce, business partners and/or its customers, clients, or employees.

4.2 Information Management: Information must be handled in accordance with the Information Classification and Management Standards S-RA-01 developed by NYC3.

5 NON-COMPLIANCE

5.1.1 City employees found to have violated this policy may be subject to disciplinary action, and in certain instances, civil or criminal penalties.

5.1.2 Any Information System that does not adhere to this policy may be taken offline until such time that a formal assessment can be performed at the discretion of the Chief Information Security Officer for the City of New York.

5.1.3 NYC Cyber Command can conduct periodic audits to review the security posture of any Information System, as well as the information provided during the Data Classification Process.

6 AUTHORITY

The New York City Cyber Command, in collaboration with the New York City Department of Information Technology and Telecommunications, issues this Information Classification and Management Policy pursuant to Mayoral Executive Order 28 of 2017. The Mayor's Office of Information Privacy was consulted and contributed to the promulgation of this policy. This policy applies to any technology system owned, maintained, and/or operated by any agency of the City of New York ("City Agency") and to any agency that connects a device or network to any such system ("Non-City Agency"). The requirements contained here are binding on all City and Non-City Agency heads.

7 REFERENCES

7.1.1 National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53, rev. 4, "Recommended Security Controls for Federal Information Systems"

7.1.2 National Institute of Standards and Technology (NIST) Special Publication 800-60 Volume I Revision 1

7.1.3 National Institute of Standards and Technology (NIST) Special Publication 800-18 Revision 1 - Guide for Developing Security Plans for Federal Information Systems