Policy: Data Classification Policy	Information Security & Privacy 01.103

New Hampshire Department of Health and Human Services
Bureau of Human Resource Management

Effective Date: 08/6/2020 Approved:
Last Revision:



Lori A Weaver, Deputy Commissioner
Date: 8/7/2020

Last Reviewed by Information Services: 06/18/2020

Regulatory References:	Other References:
Regulation(s): Statute(s): RSA 91-A Admin Rules(s): PART Per 1002 DISCIPLINE	NIST 800-53 DHHS Confidentiality Policy DHHS Data Classification Procedure DoIT Data Classification Policy

Section 1 - PURPOSE OF POLICY

1.1. The purpose of this policy is to establish the requirements for classifying the Department of Health and Human Services (DHHS) data based on its level of sensitivity, value and criticality. Data classification is used to align levels of protection to safeguard the security and privacy of data and ensure compliance with state and federal laws and regulations.

Section 2 – DEFINITIONS

2.1. Business/Data Owners - Individuals accountable for adhering to the DHHS information security and privacy policies within their respective business area and associated services.

2.2. Confidential Data – For the purposes of this policy, "Confidential Data" means all non-public information owned, managed, created, received from, or on behalf of, the Department that is protected by information security, privacy or confidentiality rules, and state and federal laws. This information includes but is not limited to derivative data, Protected Health Information (PHI), Personally Identifiable Information (PII), Federal Tax Information, Social Security Administration, and CJIS (Criminal Justice Information Services) data. Confidential data is classified as DC-3 or DC-2 data.

2.3. Contractor – Any individual or entity performing services for the Department under a written agreement, including the employees and sub-contractors of the individual or entity.

2.4. Data Classification – is the process to consistently organize and manage data based on its level of sensitivity, value and criticality should that data be accessed, disclosed, altered

or destroyed without authorization. Data classification determines the levels of protection and controls required to safeguard the confidentiality (undisclosed), integrity (unaltered) and availability (accessible) of that data, reducing the risk of a data events or breaches with financial, legal and reputational implications.

2.5. Data Governance – is a matrixed program that consists of all Data Stewards, Information Service Leads and the Data management Group. It was created to assure the consistency, confidentiality, integrity, and availability of New Hampshire data while promoting data sharing and interoperability.

2.6. Data Steward – Department employees identified by the Division Directors has having responsibility for the lifecycle data management of the business processes such as access, storage, retention, distribution or exchange of data.

2.7. Department – Department of Health & Human Services.

2.8. Department Employee – An individual working in an authorized Department position number.

2.9. Department Staff – Department employees, contractors, unpaid interns, and volunteers.

2.10. DoIT – The New Hampshire Department of Information Technology.

2.11. Non-public: Regulated Confidential Data – Data regulated by State or Federal law and/or agreement. It shall also have the same meaning as "Confidential Data" as defined in this policy and is classified as "level 3" data (DC-3). For further information on data classification, refer to the Department's Data Classification Policy and Table.

2.12. Non-public: Restricted Data - Data not subject to release under Right to Know request per NH RSA Chapter 91:A Such data may be released to an individual or entity subject to proper authorization, redaction or suppression and is classified as "level 2" data (DC-2). For further information on data classification, refer to the Department's Data Classification Policy and Table.

2.13. Public: Non-published Data - Data subject to release under Right to Know request per RSA Chapter 91:A is classified as "level 1" data (DC-1). For further information on data classification, refer to the Department's Data Classification Policy and Table.

2.14. Public: Published Data - Data for which there is no expectation for privacy or confidentiality and therefore has been made available to the general public and is classified as "level 0" data (DC-0). For further information on data classification, refer to the Department's Data Classification Policy and Table

2.15. Right-to-Know – A New Hampshire statute (RSA 91-A) that affects every aspect of government in the state of New Hampshire. The intent of the Right-to-Know (RTK) law is to guarantee that the public has access to public records of all governmental bodies in the state of New Hampshire. To read the RTK law or to review exemptions to this law go to http://www.gencourt.state.nh.us/rsa/html/VI/91-A/91-A-5.htm.

2.16. Supervisor – The Department staff's immediate supervisor/Point-of-Contact or a person at a higher supervisory level within the Department staff's chain of management within the Department

2.17. System Owners - Individuals within business operations responsible for safeguarding data and the efficient management and operations of technology systems and applications.

2.18. Unpaid Interns – A student who is enrolled in a post-secondary educational institution for the educational benefit of the student and has signed an unpaid internship agreement with the Department.

2.19. Volunteers –An individual who freely offers to undertake a service for the Department without compensation of any kind.

Section 3 - SCOPE

3.1. This policy applies to all Department staff.

Section 4 - POLICY STATEMENT

4.1. Data classification is the process to consistently organize and manage data based on its level of sensitivity, value and criticality should that data be accessed, disclosed, altered or destroyed without authorization. Data classification determines the levels of protection and controls required to safeguard the confidentiality (undisclosed), integrity (unaltered) and availability (accessible) of that data, reducing the risk of a data events or breaches with financial, legal and reputational implications. The process of data classification identifies:

- What data exists and where it is stored
- Data ownership and responsible points of contact (data stewards)
- Business criticality (function) and sensitivity (impact)

4.2. All data must be classified into one of the four categories in the below Data Classification Table based on data value, sensitivity, and impact as determined through the data classification procedure located at http://intranet/info-sec/data-class.html

Category		Category Score	Impact Loss	Description
Non-Public	Regulated Confidential	DC-3	High	Data regulated by State or Federal law and/or agreement.
	Restricted	DC-2	Moderate	Data not subject to release under Right to Know request per RSA Chapter 91:A. Such data may be released to an individual or entity subject to proper authorization, redaction or suppression.

Category		Category Score	Impact Loss	Description
Public	Non-Published	DC-1	Low	Data subject to release under Right to Know request per RSA Chapter 91:A.
	Public	DC-0	None	Data for which there is no expectation for privacy or confidentiality and therefore has been made available to the general public.

With the multiple data sources within Department the central aggregation of data classifications is required for security compliance. All data classification results will be maintained by the information services bureau in a secure location. This central repository provides Information Security, the Data Governance Group, the Incident Response Team, and Data Stewards with information required to oversee data classification efforts, determine impact from incidents and outages, assist with the prioritization of recovery efforts, and oversee regulatory compliance, planning, and decision-making to further reduce risks and costs.

4.3. Data classification requires on-going management and routine review to ensure the assigned classification remains consistent with impact risk, regulatory requirements, agreements, data quality, and use or maintenance of that data. Each data classification must be reviewed and updated annually at a minimum, and when system or relevant regulatory requirements change.

Section 5 - RESPONSIBILITY

5.1. Business/Data Owners are responsible for ensuring business compliance with the policy.

5.2. The Bureau of Information Services is responsible for developing, maintaining, and monitoring this policy.

5.3. Department Directors, Administrators, and Supervisors are responsible for enforcing this policy.

5.4. Department staff are responsible for complying with this policy.

Section 6 - SANCTIONS

6.1. Any Department employee found to have violated this policy shall be subject to appropriate discipline as provided by the Administrative Rules of the Division of Personnel.

6.2. Contractors, unpaid interns, and volunteers must be subject to appropriate monitoring and compliance with this policy as provided by the contract or agreement with the Department, or as permitted by law.

Section 7 - DISTRIBUTION

7.1. Department policies are posted on the Department Intranet under the Policies and Procedures Section.

7.2. Human Resources will notify all Department staff via e-mail when new policies are posted to the Intranet.

7.3. Supervisors responsible for Department staff that DO NOT have access to email must bring this information to their attention as soon as possible.

7.4. Policies involving information security will also be posted to the Department's website.