



# State of New Hampshire Department of Information Technology Office of the Chief Information Security Officer (CISO)

## Data Classification Policy

### **PURPOSE**

The purpose of this policy is to differentiate the treatment of data based on its data classification.

### **APPLICABILITY**

The policies, standards, procedures, and guidelines included in the SISM apply to all Departments, Agencies, Commissions, Boards, Bodies, or other instrumentalities of the Executive Branch of New Hampshire State Government, hereinafter referred to as: agencies, the Executive Branch, the SoNH, or the State. All Executive Branch full-time and part-time employees, temporary workers, volunteers, interns, contractors, and those employed by contracted entities - collectively referred to as "SISM Users" - are governed by and responsible for complying with the policies and standards regardless of agency, location, or role.

### **1.1. SECURITY CONTROLS**

This policy has been mapped to the applicable standard and the standard tags are contained in the procedure's metadata and listed here:

NIST SP 800-53 Rev. 5 Controls:

- RA-2 Security Categorization

### **2. ROLES AND RESPONSIBILITIES**

- Agencies
- Agency Security
- Legal Counsel
- Privacy Officers

Agencies shall classify all information generated, collected, stored, processed, or transmitted by State of New Hampshire information systems in accordance with all applicable statutory, regulatory, and contractual requirements and according to the information's sensitivity, along with an assessment of risks associated with the potential loss of confidentiality, integrity, availability, or privacy.

The following data classification schema is to be used when classifying data.

- **Public:** Information that is intended, or required, to be shared with the public.
- **Sensitive:** Information critical to on-going operations which should not be copied, shared, or removed outside of the Organization without authority.
- **Confidential:** Sensitive information that is used or held by an Agency. Considerable loss or harm could occur because of unauthorized access, use, or disclosure of this information.
- **Restricted:** Highly sensitive information that is used or held by an Agency. Statutory or regulatory penalties, notification provisions, or other mandates could result if the information is accessed, used, or disclosed in an unauthorized manner.

NIST SP 800-53 Rev. 5 Controls: RA-2

## DATA CLASSIFICATION AND SECURITY CATEGORIZATION CONSIDERATIONS

The considerations listed below must be evaluated by Agencies when assigning security categorizations to their information assets and determining the impact should a loss of confidentiality, integrity, availability, or privacy be realized.

Legal, Regulatory, Contractual, and Policy Compliance - Various federal and state laws, regulations, contracts, and policies mandate the protection of personal information from unauthorized access, use, or disclosure. Questions regarding laws and regulations that apply to specific Agencies and the information they collect, store, process, or output should be directed to the Agency's Legal Counsel (Office of the Attorney General).

**Personally Identifiable Information (PII)** - [NIST SP 800-171](#) defines PII as any information about an individual maintained by an Agency, including:

- Any information that can be used to distinguish or trace an individual identity, such as name, social security number, date and place of birth, mother's maiden name, or biometric records.
- Any other information that is linked or linkable to an individual, such as medical, educational, financial, and employment information.

Examples of PII include, but are not limited to:

- Name, such as full name, maiden name, mother's maiden name, or alias Personal identification number, such as social security number (SSN), passport number, driver's license number, taxpayer identification number, patient identification number, and financial account or credit card number.
- Address information, such as street address or email address.
- Asset information, such as Internet Protocol (IP) or Media Access Control (MAC) address or another host-specific persistent static identifier that consistently links to a particular person or small, well-defined group of people.
- Telephone numbers, including mobile, business, and personal numbers.

- Personal characteristics, including photographic image (especially of face or other distinguishing characteristic), x-rays, fingerprints, or other biometric image or template data (e.g., retina scan, voice signature, facial geometry).
- Information identifying personally owned property, such as vehicle registration number or title number and related information.
- Information about an individual that is linked or linkable to one of the above (e.g., date of birth, place of birth, race, religion, weight, activities, geographical indicators, employment information, medical information, education information, financial information).

**SENSITIVE PERSONALLY IDENTIFIABLE INFORMATION (SPII)** - Personal information, which if lost, compromised, or disclosed without authorization, could result in substantial harm, embarrassment, inconvenience, or unfairness to an individual.

**CRIMINAL JUSTICE INFORMATION** - is the term used to refer to all the FBI Criminal Justice Information Services provided data necessary for law enforcement and civil Agencies to perform their missions including, but not limited to biometric, identity history, biographic, property, and case/incident history data. The following categories of CJI describe the various data sets housed by the FBI CJIS architecture:

- Biometric Data - data derived from one or more intrinsic physical or behavioral traits of humans typically for the purpose of uniquely identifying Individuals from within a population. Used to identify Individuals, to include fingerprints, palm prints, iris scans, and facial recognition data.
- Identity History Data - textual data that corresponds with an individual's biometric data, providing a history of criminal and/or civil events for the identified individual.
- Biographic Data - information about Individuals associated with a unique case, and not necessarily connected to identity data. Biographic data does not provide a history of an individual, only information related to a unique case.
- Property Data - information about vehicles and property associated with crime when accompanied by any personally identifiable information (PII).
- Case/Incident History - information about the history of criminal incidents.

**FEDERAL TAX INFORMATION (FTI)** - FTI consists of federal tax returns and return information (and information derived from it) that is in the Agency's possession or control which is covered by the confidentiality protections of the [Internal Revenue Code](#) (IRC) and subject to the IRC 6103(p)(4) safeguarding requirements including IRS oversight. FTI includes return or return information received directly from the IRS or obtained through an authorized secondary source, such as Social Security Administration (SSA), Federal Office of Child Support Enforcement (OCSE), Bureau of the Fiscal Service (BFS), or Centers for Medicare and Medicaid Services (CMS), or another entity acting on behalf of the IRS pursuant to an IRC 6103(p)(2)(B) Agreement.

FTI includes any information created by the recipient that is derived from federal return or return information received from the IRS or obtained through a secondary source.

**ELECTRONIC PROTECTED HEALTH INFORMATION (EPHI)** – Electronic Protected Health Information (PHI) consists of any information about health status, provision of health care, or payment for health care that

can be linked to an individual. PHI refers to all “individually identifiable information” held or transmitted by the State Entities or its business associates in any form or media, whether paper, electronic or oral. “Individually identifiable health information” is information, including demographic data, which relates to:

- The individual’s past, present, or future physical or mental health or condition,
- The provision of health care to the individual, or
- The past, present, or future payment for the provision of health care to the individual,
- The individual's identity, or for which there is a reasonable basis to believe it can be used to identify the individual.

**SOCIAL SECURITY ADMINISTRATION PROVIDED INFORMATION** – is information that is obtained from the Social Security Administration (SSA). This can include a Social Security number verification indicator or other PII data.

**PAYMENT CARD INDUSTRY (PCI) DATA SECURITY STANDARD (DSS) INFORMATION** – PCI DSS applies to the transmission, storage, or processing of confidential credit card data. This data classification includes credit card magnetic stripe data, card verification values, payment account numbers, personally identification numbers, passwords, and card expiration dates.

Potential Harm to Individuals - Agencies must consider any potential harm or adverse impact that the compromise of information may have on the parties to whom the information pertains.

**Agency Mission and Business Objectives** - Agencies must consider their mission and business objectives when assigning information classifications. Certain Agencies may be obligated to share as much of their data as possible with the public or other outside Agencies while others may be under the strictest constraints in ensuring that their data is protected against any exposure whatsoever. In either case, while it is incumbent on the Agency to ensure that those objectives are met, adequate controls need to be in place and in effect to address confidentiality, integrity, availability, and privacy.

**Information System Dependencies/Connections and Aggregation/Commingling of Information** - Agencies must consider the risks associated with information system dependencies and connections to other systems when classifying information. Low-sensitivity information protected by the minimum required controls in isolation must implement more restrictive controls when connected to systems containing high-sensitivity information. Information Owners must consider the sensitivity of information types in the aggregate when assigning classifications.

The confidentiality of an individual’s first and last name is not considered High Impact information on an isolated system. When connected to, combined with, or commingled on, a system that includes other identifiers such as a social security number, the aggregate of the information requires classification as High Impact, highly sensitive and requires appropriate controls necessary to ensure the confidentiality of the information is maintained.

**Information Sharing Agreements, Memorandums of Understanding, and Contractual Requirements** - Information Sharing Agreements, Memoranda of Understanding (MOU), grants, contracts, and other

written agreements between Agencies and external entities may include agreements regarding information access, sharing, use, disclosure, and maintenance of information, as determined by the information classification of the Information Owner. The recipient Organization's information risk classification must align with any such requirements.

Additionally, if an agreement states that the recipient Agency may further share the information, the subsequent recipients must adhere to the requirements of the original classification.

**Intellectual Property** - Agencies must consider any intellectual property rights owned by an entity other than the State Agency, when determining information risk classification assignments.

**Information Lifecycle** - Agencies must consider the risk classification of information throughout their lifecycle as changes may occur prompting changes to the classification and the associated security controls. As an example, contract bids prior to award are classified as High Impact information. Post award, the risk classification of contract bids may be lowered and thus require fewer protective controls regarding confidentiality.

**Metadata** - Agencies must consider metadata when classifying information. Metadata is often referred to as "data about data". Metadata describes or supplements the information and may be either separate from or embedded within documents, records, or objects. Examples of metadata include filename, creation date, file size, author, etc. While metadata may not be readily readable, the sensitivity of the metadata alone or in combination with the information, needs to be considered.

Agencies should consult with Agency Security and Privacy Officers and Legal Counsel when determining data classifications. A non-exhaustive list of examples of commonly held data and their classifications are included in the table.

RESTRICTED	CONFIDENTIAL	SENSITIVE	PUBLIC
Federal tax information received from, or derived from, the IRS or secondary sources (IRS Pub. 1075)	Pension/Retirement benefit information (actual amounts)	Agency policies, procedures, and/or standards	Public-facing website content
Protected Health Information (HIPAA/HITECH)	Personal demographics (race, place of birth, weight, religion)	Training materials	Publicly distributed information
Social Security numbers	Unpublished information about Agency Personnel such as home telephone numbers and home addresses used for emergency contact	Internal meeting information	Meeting agendas and minutes from public meetings
Debit or credit card numbers	All information exempts from disclosure pursuant to New Hampshire Law	Direct telephone line numbers to staff	Brochures
Driver's license information or State identification card Information	Information received from and/or about a business (tax information, business plans)		Press releases
Bank account numbers or information with personal identification numbers (PINs) or passwords	Security plans, network architecture, etc.		Agency contact information
Passport numbers			
Biometric Identifiers			
Child welfare and legal information about minors			

NIST SP 800-53 Rev. 5 Controls: RA-2

### ASSIGNING SECURITY CATEGORIZATIONS

Agencies shall assign security categorizations that represent the impact level should an information system or asset suffer a loss of confidentiality, integrity, or availability. The impact level is a function of the sensitivity and criticality of the system or asset.

Agencies shall use the following impact levels when assigning security categorizations:

**Low:** The loss of confidentiality, integrity, or availability that could be expected to have a limited adverse effect on Agency operations, Agency assets, Individuals, other Organizations, or the State of New Hampshire, such as:

- Causes a degradation in mission capability to an extent and duration that the Organization can perform its primary functions, but the effectiveness of the functions is noticeably reduced.
- Results in minor damage to Agency assets.
- Results in minor financial loss.
- Results in minor harm to Individuals.

**Moderate:** The loss of confidentiality, integrity, or availability that could be expected to have a serious adverse effect on Agency operations, Agency assets, Individuals, other Organizations, or the State of New Hampshire, such as:

- Causes a significant degradation in mission capability to an extent and duration that the Agency can perform its primary functions, but the effectiveness of the functions is significantly reduced.
- Results in significant damage to Agency assets.
- Results in significant financial loss.
- Results in significant harm to Individuals that does not involve loss of life or serious life-threatening injuries.

**High:** The loss of confidentiality, integrity, or availability that could be expected to have a severe or catastrophic adverse effect on Agency operations, Agency assets, Individuals, other Organizations, or the State of New Hampshire, such as:

- Causes a severe degradation in mission capability to an extent and duration that the Agency can perform its primary functions, but the effectiveness of the functions is significantly reduced.
- Results in major damage to organizational assets.
- Results in major financial loss.
- Results in severe or catastrophic harm to Individuals involving loss of life or serious life-threatening injuries.

Systems shall inherit the categorizations of the information which they generate, store, process, or transmit, and are to be protected; accordingly.

If more than one categorization could apply to a system or asset, the highest level (most restrictive) shall be applied.

The following Security Categorization Matrix can be used to determine the security categorizations of information assets.

SECURITY CATEGORIZATION MATRIX GUIDE		SENSITIVITY			
		RESTRICTED	CONFIDENTIAL	SENSITIVE	PUBLIC
CRITICALITY/ AVAILABILITY	MISSION CRITICAL	HIGH	HIGH	HIGH	HIGH
	BUSINESS CRITICAL	HIGH	HIGH	MODERATE	MODERATE
	NON- CRITICAL	HIGH	MODERATE	LOW	LOW

When assigning security categorizations to information assets, Agencies should document the categorization results, including supporting rationale for the categorization. Agencies must ensure all assets, within an authorization boundary to which a given asset is connected, have required controls applied in accordance with its security categorization.

Security categorization processes carried out by Agencies facilitate the development of inventories of information assets and mappings to specific information system components where information is processed, stored, or transmitted. Security categorizations are key elements and should be included in service level agreements and other contract vehicles with service providers.

NIST SP 800-53 Rev. 5 Controls: RA-2

### 3. REFERENCES

- NIST SP 800-53 Rev. 5 Standard which can be found at:  
<https://csrc.nist.gov/publications/detail/sp/800-53/rev-5/final>.



**REVISION HISTORY:**

The New Hampshire State Chief Information Security Officer (CISO) shall update the Revision History table below to document all new or substantive changes in alignment with NHS0168 DoIT's Control of Documented Information Policy.

The effective date of any added, changed, updated, or deleted policy shall be the date of entry in the Revision History table.

Version	Date	Policy/ Standard #	Description	CISO Signature
1.0	8/5/22	All	Initial issue of Statewide Information Security Manual (SISM) using NIST 800-53 Rev. 5 Moderate Baseline.	KLW-8/5/2022
2.0	9/7/23	All	Reviewed, no change to content; update to new template as stand-alone policy.	KLW-9/7/23