

INFORMATION CLASSIFICATION OVERVIEW

What is it?

Information classification is an on-going risk management process that helps identify critical information assets – data, records, files - so that appropriate information security controls can be applied to protect them. It is the cornerstone of an effective and efficient business-aligned information security program.

Your agencies retain a wide variety of information assets, many of which are sensitive and/or critical to your mission and business functions and services. Information is being accessed through, and maintained in, a wider variety of formats and environments. **If you do not know what information assets you have, their value to the business, and where they are stored, how can you assure they are protected properly?**

Why is it important?

We are obligated to protect the information that New York State (NYS) citizens and business partners have entrusted to our care. Agency heads are ultimately responsible for assuring this occurs. Loss of information can lead to operational and productivity impact, compliance, legal, financial and reputational risk and potential loss of public trust. It is far less expensive to apply resources toward ensuring appropriate controls, than to experience a breach and have to notify affected parties and remediate after-the-fact.

Not all information assets require the same level of protection. Information classification helps determine the proper levels of protection and selection of appropriate controls.

Who is responsible for information classification?

Protecting information is a shared responsibility that requires support of your entire organization. This responsibility begins at the top, with executive-level support. It is important to place the responsibility for leading your efforts to identify and classify agency information assets with an individual who has a sound understanding of your business. This person should be in a managerial position.

Each business unit should be involved in identifying and classifying their own data. Information classification is best managed as a collaborative effort with a cross functional team who can mentor information owners and facilitate the decision making process.

Information owners are responsible for determining their information's classification, and how and by whom the information is used. The information owner works with subject matter experts, including program managers, Counsel's Office, the Records Management Officer and Information Security Officer, who have specific knowledge about the information to assist with the classification and reduce individual subjectivity.

Where does the Office of Information Technology Services (ITS) come in?

In most cases, ITS is the custodian of agency information, and will be responsible for implementing appropriate technical controls. *Information custodians* are people, units or organizations responsible for implementing appropriate controls based on the agency's classification determination. The ITS Enterprise Information Security Office (EISO) will be conducting assessments to ensure agency and ITS compliance with information classification and control standards, and has a number of resources (see below) to help agencies with the process.

Where do I start?

Inventory your information assets. Focus on your critical business functions first and identify the underlying information assets. Target areas where sensitive and critical information is most likely to live. Classify your information assets. Ensure proper controls are in place based on classification.

What resources are available to me?

In addition to the information classification requirements contained in the NYS [Information Security Policy](#), the ITS EISO has published an [Information Classification Standard](#) that outlines the classification process and includes supplemental guidance to walk an agency through it. The [Information Security Controls Standard](#) identifies the appropriate baseline controls for each classification level in easy-to-understand charts, with non-technical explanations and details. The [Secure System Development Lifecycle \(SSDLC\) Standard](#) supports information classification in that it makes sure that development of new systems and/or applications includes a required information classification step.

Online Information Classification Training is available on the ITS EISO website.

The Information Asset Classification System (IACS) tool developed by ITS EISO, is a secure, web-based application that will help your agency manage information classification efforts. It automates the process outlined in the Information Classification Standard. It has a 'TurboTax'-like look and feel, and efficiently walks the user through a set of predefined questions to determine an asset's classification. 'Traffic light' colors (i.e., red - high, yellow - moderate, and green - low) display the classification in real-time as the questions are answered. Once the classification is determined, the user is presented with baseline controls that are needed to protect the asset. IACS also allows for a gap analysis of controls for each classified information asset.

A state-wide effort aimed at classifying common data sets in use across state agencies ([General Retention and Disposition Schedule for New York State Government Records](#)), such as personnel records and security logs, was undertaken to avoid duplicating efforts. The guidance from this effort has been integrated into templates within the IACS tool to facilitate classification of these records.

Information Classification Toolkit

This one-page overview and all other resources to support your information classification efforts are available online, in one convenient location. <http://www.its.ny.gov/eiso/infoclass>

- *Information Security Policy*
- *Information Classification Standard*
- *Information Security Controls Standard*
- *Secure System Development Life Cycle (SDLC) Standard*
- *Online Information Classification Training*
- *Information Asset Classification System (IACS) General Information, Access Request Form, and User Guide*
- *Recommended Classifications of Common Data Sets*

For further information

Contact the Office of Information Technology Services Enterprise Information Security Office at 518-242-5200 or eiso@its.ny.gov.

