State of Oregon
Information Asset Classification Methodology

Information Asset Classification

The purpose of statewide policy 107-004-050 (effective 7/30/2007) is to ensure State of Oregon information assets are identified, properly classified, and protected throughout their lifecycles. Information, like other assets, must be properly managed from its creation to disposal. As with other assets, not all information has the same value or importance to the agency and therefore information requires different levels of protection. Information asset classification and data management are critical to ensure that the state's information assets have a level of protection corresponding to the sensitivity and value of the information asset.

The provisions of the policy collectively apply to all information assets, including but not limited to paper, electronic, and film. The term "information asset" is not used within this framework to refer to the technology that is used to store, process, access and manipulate the information. Information technology assets that are not considered information assets include software (including application and system software), development tools and utilities, associated licenses, physical assets such as computing equipment, storage media, power supplies, and other technical equipment that may impact the confidentiality, availability or integrity of information resources.

The objective of the information asset classification initiative is to develop and implement processes that allow an organization to continually assess and classify its information assets and provide information asset classification plans for assessment purposes. Information asset classification allows an organization to:

- Continually assess what types of precautions must be taken to ensure the confidentiality, integrity, and availability of its information assets related to their value.
- Collect documentation on its information assets:
  - Compliance requirements
  - Information owner
  - Associated business function, such as business continuity planning
  - Archive and retention requirements

There are six maturity stages of the information asset classification initiative:

- **Stage 0 –** No information assets are classified or assets are randomly classified.
- **Stage 1 –** Assets are classified at a high level or organizational level, assets are not identified.
- **Stage 2 –** Processes are developed and implemented, allowing assets to be classified in detail.
- **Stage 3 –** New assets are classified in detail.
- **Stage 4 –** Legacy assets are classified in detail.
- **Stage 5 –** Assets are classified, and processes exist that allow for asset reassessment and new asset classification.

Based on this model, it is likely that many state agencies were at Stage 0 at the time the statewide Information Asset Classification policy was approved. While Stage 5 is the ultimate goal, it is anticipated with the proper support and guidance, most agencies will be able to reach Stage 1 within the earliest timeframes outlined in the policy (July 2008) and be able to reach Stage 2 when the agency has completed its initial asset classification.

Where does an organization start?

1. Determine the organization's information asset classification maturity level.
2. Develop documented methodologies and mechanisms for identifying and classifying assets.
3. Determine short-term and long-term goals to demonstrate constant improvement.
4. Synchronize information asset classification efforts with other business-related activities such as business continuity planning or document retention initiatives.

A five-phase approach is recommended for agency implementation:

1. Management education – informing managers of the importance of information asset classification as the foundation for information security and protecting the information the agency is entrusted with. For an example of an awareness presentation, see http://oregon.gov/DAS/EISPD/ESO/IAC.shtml.
2. Implementation strategy – developing an agency strategy for implementing the provisions of the information asset classification policy. For an example of a comprehensive information asset classification framework, refer to the Queensland (Australia) Government document located at http://oregon.gov/DAS/EISPD/ESO/IAC.shtml.
3. Employee education – informing employees of the agency's asset classification scheme and the proper steps and procedures for handling information assets. For an example of an awareness presentation, see http://oregon.gov/DAS/EISPD/ESO/IAC.shtml.
4. Implementation – putting the strategy into practice and beginning the process of identifying, classifying and protecting agency information assets.
5. Maintenance – a program of continuous review of asset classifications, ensuring new information assets are properly classified, and continuous awareness and training of agency employees.

The following methodology is provided to assist agencies in their information asset classification efforts. This information is presented as considerations or guidelines. Examples have been provided of how others have approached tasks associated with information asset classification. For access to the resources mentioned in this methodology document and other examples of best practices, templates, and sample documents, see http://oregon.gov/DAS/EISPD/ESO/IAC.shtml.

Classification Methodology

1.0	**Identify information assets**
	Information assets come in many forms, including but not limited to: • Paper • Electronic • Digital • Images • Voice mail
	Examples of information assets include, but are not limited to: • Employee-related information including employee records, job applications, and records of interview; • Procurement records such as RFP specifications, evaluation of proposals, contracts, pricing details, and performance reports; • Agency information such as policies, strategic plans, correspondence, legal advice, financial and audit reports, system documentation, user manuals, training material, operational and support procedures, business continuity plans, system architecture drawings, and risk analyses; • Client information including service level agreements, service contracts, and client contact records; and • Customer information including personal identity information collected to issue licenses or certifications, report income, and track education credits.
	In order to facilitate the classification of information assets and allow for a more efficient application of controls, it may be desirable to group like information together. It is important to ensure that the grouping of information assets for classification is appropriate. A broad grouping may result in applying controls unnecessarily as the asset must be classified at the highest level necessitated by its individual data elements. A narrow grouping allows for more precise targeting of controls; however, as there are more information assets to classify, this increases the complexity of the classification and the management of controls
	Information assets may be defined as **mission-based (or function-based)** information. Mission-based information types are, by definition, specific to individual departments and agencies or to specific sets of departments and agencies. Much government information and many information systems are used directly for the provisioning of services. One approach to establishing mission-based information types at an agency level is to begin by documenting the agency's business and mission areas.
	Much government information and many systems are not employed directly to provide services to citizens, but are primarily intended to manage resources or support delivery of services. These include the support functions necessary to conduct government (support delivery of services) and resource management functions that support all areas of government's business (management of resources). Services **delivery support** functions are the day-to-day activities necessary to provide critical policy, programmatic, and managerial foundation that support state government operations (controls and oversight, regulatory development, planning and resource allocation, internal risk management and mitigation, public affairs, revenue collection, legislative relations, general government). The **government resources management** information business area includes the back office support activities that enable government to operate effectively (human resources, administrative management, information technology management, financial management, supply chain management).
	Where information is identified, consider legislation, regulations, policy compliance, and/or contractual obligations that affect the management of the information.
	Where practical, leverage other business initiatives such as business continuity planning/disaster recovery planning, implementation of enterprise policies and initiatives, and implementation of new lines of business and incorporate information asset identification, classification and handling methodologies to protect newly identified information assets.

2.0	**Identify the owner of the information assets**
	All information assets should have identified information owners established within the agency's lines of business. These information owners are responsible for ensuring the agency: • Creates an initial information asset classification, including assigning classification levels to all data; • Approves decisions regarding controls, access privileges of users, and ongoing decisions regarding information management; • Understands who is using the information and how it is being used; • Ensures the information is regularly reviewed for value and updated to manage changes to risks due to new threats, vulnerabilities or changes in the environment; • Supports and understands information sharing agreements; • Performs periodic reclassification based on business impact analyses, changing business priorities or new laws, regulations and security standards; and • Follows state archive record retention rules regarding proper disposition of all information assets.
	Information should be classified by the information owner or delegate at the earliest possible opportunity and as soon as the originator or owner is aware of the sensitivity of the information asset. Consideration must be given to stakeholders, users, and consumers of the information with regard to accessibility and business process changes that may adversely affect their respective business processes or consumer needs.
	Information owner questions: • What is the information? • Where is the information used? • When is the information needed and not needed? • Why is the information needed? • How is the information used?
	In the case of information externally generated and not otherwise classified, the agency officer who receives the information should approach his or her own agency information owner or delegate to classify the information and guide its control within the agency.

3.0	**Conduct an impact assessment of information assets**
	Once information assets are identified, conduct an impact assessment on the value of the asset to the organization and any risks associated with its disclosure. Include in the assessment any known legislation, regulations, policy compliance, and contractual obligations affecting the management or use of the information.
	An example of a risk assessment methodology can be found at http://oregon.gov/DAS/EISPD/ESO/IACCoP/RiskAssmtTool.doc.

	Identify threats (http://oregon.gov/DAS/EISPD/ESO/IACCoP/ThreatsConcerns.doc) to assets and determine the likelihood of them occurring.
	• Identify threats as if there were no security measures in place
	• Explore causes, the extent of affected information assets, and possible consequences
	  ○ Express consequences in a manner that reveals the affected security objectives
	  ○ Determine any possible actions that will mitigate the risk
	• Determine the likelihood of the threat occurring
	  ○ Take into account any existing security measures that may mitigate the risk
	• Determine the classification level of the information asset

	Classification decisions are not strictly limited to a consideration of the threat to security. The costs of

	additional steps and additional resources needed to mitigate the risk, cost of not mitigating risk, and whether there is an information exchange associated with the information asset also should be considered. Agencies must determine the classification level based on a balanced approach.

4.0	**Determine the classification of the information asset**
	Once assets are identified and a risk assessment completed, assign information asset classifications to the assets.
	Information assets should be classified according to business need and findings from the impact assessment. Business needs vary and similar information assets may be classified differently from agency to agency. One agency may classify their network diagrams as restricted and another agency may classify their network diagrams as limited based on the level of detail provide and the business need.
	The highest classification level determined by the impact assessment must be applied to that asset.
	When identifying the proper classification level of an asset, consider the implications of exchanging the information internally and with external partners. How would you expect your exchange partners to handle and protect those assets?
	Published classification is low-sensitive information. Information that is not protected from disclosure, that if disclosed will not jeopardize the privacy or security of agency employees, clients and partners. This includes information regularly made available to the public via electronic, verbal or hard copy media. Examples: • Press releases • Brochures • Pamphlets • Public access Web pages • Materials created for public consumption
	Limited classification is sensitive information that may not be protected from public disclosure but if made easily and readily available, may jeopardize the privacy or security of agency employees, clients, and/or partners. Each agency shall follow its disclosure policies and procedures before providing this information to external parties. Examples: • Enterprise risk management planning documents • Published internal audit reports • Names and addresses that are not protected from disclosure
	Restricted classification is sensitive information intended for limited business use that may be exempt from public disclosure because, among other reasons, such disclosure will jeopardize the privacy or security of agency employees, clients, partners or individuals who otherwise qualify for an exemption. Information in this category may be accessed and used by internal parties. External parties requesting this information for authorized agency business must be under contractual obligation of confidentiality with the agency (for example, confidential/non-disclosure agreement) prior to receiving it. Examples: • Network diagrams • Personally identifiable information • Other information exempt from public records disclosure
	Critical classification is information that is deemed extremely sensitive and is intended for use by named individual(s) only. This information is typically exempt from public disclosure because, among other reasons, such disclosure would potentially cause major damage or injury up to and including death to the named individual(s), agency employees, clients, partners or cause major harm to the agency. Examples: • Regulated information with significant penalties for disclosure, such as information covered under HIPAA or IRS regulations • Information that is typically exempt from public disclosure

5.0	**Document classified information assets**
	Once the appropriate classification is identified, the asset and its classification must be documented.
	Establish and maintain a register(s) to record the classification of each information asset. Determine at what organizational level the register(s) will be maintained.
	An example of a register that also identifies retention schedules can be found at http://oregon.gov/DAS/EISPD/ESO/IACCoP/DataClassList_example.doc .
	The register is ideally maintained in a central location and should cover all security classified information assets of an agency so it can be readily accessed.
	As a minimum, the register(s) should include: • Name or unique identifier of asset or group of assets • Description of information asset (i.e. what type of information it contains); • Location of information asset; • Information owner; • Classification of the information asset; • Date of classification with details of the authority for the classifier (i.e. who approved the classification) • Reason for the classification of the information asset (particularly important to support review and reclassification of the information asset at a later time; should include legislative, regulatory, policy or other reference where applicable, or a copy of the impact assessment date); and • Date to review classification (if known).
	The following information is desirable in the register(s) for highly sensitive or confidential information assets: • Users and usage of the information; • Number of copies in circulation and their location; and • Disposal details where information has been disposed of.
	Electronic document and records management systems generally contain functionality to record classification metadata for information they manage and may be capable of automatically populating and maintaining a security classified information register for the information they control.

6.0	**Provide education and awareness**
	The ongoing education and awareness of all employees in the importance of classifying information is critical to the success of the overall agency security environment.
	The agency should ensure that all employees who create, process, or handle security-classified information have a clear understanding of the agency classification policies and procedures and of their responsibilities.
	Meetings on information classification for employees working on sensitive projects can inform and remind those employees of sensitive information. Such meetings could also emphasize how pieces of seemingly harmless project information can be sensitive because that information, when combined with the information that is already available, can disclose sensitive information.
	Assess whether training is effective, and adapt training to address changing requirements and emerging threats.
	For a template to use for employee awareness of information asset classification, see http://oregon.gov/DAS/EISPD/ESO/IACCoP/IAC_Employees.ppt . Please note this template is meant to be

	used as a skeleton document where agencies will include agency-specific information and more detail as it best suits the needs of the agency.

7.0	**Maintain classification and conduct continuous review**
	Information owners should use the classification information register to annually review the classification of identified information assets.
	Establish practices for periodic reclassification based on business impact analysis, changing business priorities or new statutes, regulations and security standards.
	Establish procedures for adding new information types or deleting information no longer maintained by the agency.

Information Management Methodology

1.0	Exchanging classified information
	Establish contracts and agreements describing the procedures for appropriately using and adequately protecting information, and identify who is responsible for ensuring the procedures are completed.
	Develop and implement an information exchange assessment process to identify classifications for contracts and agreements.
	The use of standard labels to mark sensitive information, whether in electronic, paper or some other form, means that when documents are distributed among agencies they will be subject to consistent safeguards.

2.0	Handling classified information assets
	Information assets should be handled in a manner to protect the information asset from unauthorized or accidental disclosure, modification or loss.
	Example of handling: http://oregon.gov/DAS/EISPD/ESO/IACCoP/IACMatrix.doc
	All information assets should be processed and stored in accordance with the information asset classification levels assigned in order to protect the confidentiality, integrity, availability, and level of sensitivity.
	An agency that uses information from another agency should observe and maintain appropriate security for the classification assigned by the owner agency.
	Access to sensitive information should be granted by the information owner and audited on a periodic basis.
	Active measures and controls should be in place to limit access to sensitive information to as few persons as possible on a need-to-know basis.
	Encryption is required when sending sensitive information over an untrusted network.
	If sensitive information is combined with non-sensitive information, the file, tape, or disk that contains the combined information must be clearly labeled that "Sensitive information is included."

3.0	Labeling classified information assets
	Information should be properly labeled so that users are aware of ownership and classification.
	Information labeling can occur at a higher or aggregate level than the specific data or document level, depending on how the information is accessed. For example: • It may be more effective to label information at the folder level, screen level, application level, report level, or form level, than at the specific document level or data field level. • Any labeling strategy that effectively alerts the person accessing the information about its classification level would comply with the policy.
	Information belonging to different information asset classifications should be logically or physically separated or the aggregate information protected at the highest classification level.

4.0	Storing classified information assets
	Use the register(s) when determining which security controls are necessary to adequately secure information.
	Review current holdings of all personal information as defined by the Oregon Consumer Identity Theft Protection Act. In addition to ensuring compliance with the provisions of the Act, ensure, to the maximum

	extent practicable, the holding of such information is accurate, relevant, timely, and complete, and reduce them to the minimum necessary for the proper performance of a documented agency function. Specifically, personal information is a consumer's first name or first initial and last name in combination with any one or more of the following when the elements are not rendered unusable through encryptions, redaction or other methods, or when encrypted and the encryption key has been acquired: • Social Security number; • Driver license number or state identification card issued by the Department of Transportation; • Passport number or other United States-issued identification number; or • Financial account number, credit or debit card number, in combination with any required security code, access code or password that would permit access to the consumer's financial account.
	Also consider the current holdings of all other personally identifiable information such as home address, date of birth, place of birth, and mother's maiden name.
	Review the types of information collected, created, maintained, extracted, disposed, and archived (i.e., processed) to verify whether information is required for the proper performance of a business function or needed for a documented legal or business need.
	Store sensitive information out of sight in a lockable enclosure.
	Position or shield monitors to prevent viewing sensitive information by unauthorized parties.
	Store electronic documents containing sensitive information on secure drives only.

5.0	**Destruction of classified information assets**
	Information assets should be disposed of in a manner consistent with the information asset classification of the information and comply with established State of Oregon archive laws, rules and regulations.
	For proper destruction of information technology assets, refer to Statewide Policy 107-009-0050 on Sustainable Acquisition and disposal of Electronic Equipment (E-Waste/Recovery Policy) accessible at http://oregon.gov/DAS/OP/docs/policy/state/107-009-0050.pdf.