ENTERPRISE PRIVACY OFFICE

State of South Carolina
Data Classification Schema and Guidelines

V.2.0 (07.15.15)

admin
THE SOUTH CAROLINA
DEPARTMENT *of* ADMINISTRATION

Revision History

Update this table every time a new edition of the document is published

Date	Authored by	Title	Ver.	Notes
3/6/2015	Enterprise Privacy Office		1.3	Posted
7/15/15	Enterprise Privacy Office		2.0	Updated to provide introductory data schema section and improve examples of data types for each data classification category

DATA CLASSIFICATION PROCESS

Protecting the State's data is essentially a three-step process:

1. Locate your data (asset inventory)
2. Determine classification level (data classification)
3. Apply controls (implementation of administrative, physical, and technical safeguards)

DATA CLASSIFICATION SCHEMA

A Data Classification Schema has been developed to categorize the types of data that the State of South Carolina's agencies and institutions use and hold. An agency must know the types of data that it uses and holds, as well as who can access the data and where the data is located, in order to be able to develop the policies and procedures that are necessary to prevent the unauthorized use or disclosure of any sensitive information. The data classification schema used to complete step #2 of the data classification process listed in the previous section, is comprised of four categories:

1. **Public:** Information that is intended, or required, to be shared with the public.
2. **Internal Use:** Non-sensitive information that is used in the daily operations of an agency.
3. **Confidential:** Sensitive information that is used or held by an agency. Considerable loss or harm could occur as a result of unauthorized access, use, or disclosure of this information.
4. **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.

DATA CLASSIFICATION GUIDELINES

The Enterprise Privacy Office (EPO) created Table 1, which assigns classification levels to a number of the types of sensitive data or records that State agencies maintain. In cases where data or records do not appear in the examples listed below, a classification template can help agencies determine an appropriate classification level. This template is available at http://dis.sc.gov/resources/Pages/default.aspx.

A few notes to remember include:

Shared Drives

For each top-level folder, an individual can be assigned to identify or verify the contents of that folder. Once the contents are identified, the appropriate security controls can be applied. For example, Jim Smith is the manager of a Division shared drive. For each top-level folder, Jim can assign responsibility to an individual, who will identify the data. If a data element has not already been classified in these lists, the above referenced classification template can be used to assist in the task.

Databases

If the information contained in a database belongs to the agency, individuals should be assigned to review the database and use the guidance given above. Agencies are responsible for classifying their data, regardless of where it is physically located, as only the agency knows its business processes and what data it collects and maintains.

Applications

Regardless of where the data is physically located, the "owner" of the application should classify the data collected by the application, as only the owner of the application knows what the application collects.

Storage of Paper and Other Media

Regardless of format, data should be classified and protected according to Division of Information Security (DIS) controls. If the data contained therein is Restricted or Confidential, physical locks should protect the data. Best practice is a locked filing cabinet in a locked office. Freestanding filing cabinets containing Restricted or Confidential data, behind limited access doors, are acceptable. Consider measures that are necessary to minimize or protect data that may be contained in email, on copy machine or printer hard drives, or on portable devices.

Context

For some of the types of data or records, context will play an important part in classifying the record. For example, although a name and a photograph, grouped together, are considered Personally Identifiable Information, this may be considered Public Information if publicized in an agency newsletter but considered restricted information in another context, such as a health registry. Privacy liaisons should consult with their agency's Office of General Counsel, or their agency Director's office, for direction in these cases.

Multiple Applicable Levels

Records that cross classification levels should be protected at the higher level of security.

Aged Data

As data ages and/or is amended, it may raise or lower in classification (such as budget numbers before and after publication).

If agencies would like additional assistance, the EPO can be contacted via email at privacyoffice@admin.sc.gov.

Table 1. Examples of Data Types by Data Classification Level

RESTRICTED	CONFIDENTIAL	INTERNAL USE	PUBLIC INFORMATION
• Federal tax information received from, or derived from, the IRS or secondary sources (IRS Pub. 1075) • Protected Health Information (HIPAA/HITECH) • Individual financial information subject to GLBA • Social Security numbers • Debit or credit card numbers • Driver's license information or State identification card information • Bank account numbers or information with personal identification numbers (PINs) or passwords • Passport numbers • Child welfare and legal information about minors (juvenile justice, foster care and/or adoption) • Witness protection information • DNA record & profile contained in the State DNA database • Dates of birth (if linked to other information about a person) • Student education records • Trade secrets • Employee Identification Number (EIN) of a sole proprietor	• Biometric identifiers • Photographs of individual people • Pension/Retirement benefit information (actual amounts) • Personal demographics (race, place of birth, weight, religion) • Unpublished information about agency personnel such as home telephone numbers and home addresses used for emergency contact • All information exempt from disclosure pursuant to §30-4-40 of the SC Code of Laws (SC Freedom of Information Act) • Information received from and/or about a business (tax information, business plans) • Security plans, network architecture, etc. • Passwords	• Agency policies, procedures, and/or standards • Training materials • Internal meeting information • Direct telephone line numbers to staff • Aggregated data	• Public-facing website content • Publicly distributed information • Meeting agendas and minutes from public meetings • Brochures • Press releases • Agency contact information