OHCS Data Classification Guidelines

Asset Classification Levels

All information assets shall be classified strictly according to their level of sensitivity as follows:

Level 1, Published – This is characterized as being open public data with no distribution limitations and to which anonymous access is allowed. These data elements form information that is actively made publicly available by state government. It is published and distributed freely, without restriction. This includes information regularly made available to the public via electronic, verbal, or hard copy media.

The greatest security threat to this data is from unauthorized or unintentional alteration, distortion, or destruction of this data. Security efforts appropriate to the criticality of the system containing this data must be taken to maintain its integrity.
Examples:
Press releases
Brochures
Pamphlets
Public access web sites
Materials created for public consumption

Level 2, Limited – These data elements are the information that is made available through open records requests or other formal or legal processes. This category includes the majority of the data contained within the state government electronic databases. Direct access to this data is restricted to authenticated and authorized individuals who require access to that information in the course of performing their duties.

Security threats to this data include unauthorized access, alteration, and destruction concerns.
Examples:
Most data elements in state personnel records
Building code violations data
Driver history records
Collective bargaining data
Employment & training program data
Federal contracts data
Firearm permits data
Historical records repository data
Real estate appraisal data
Occupational licensing data
Personnel data
Published internal audit reports
Telephone numbers
Email addresses
Date of birth
Enterprise risk management planning documents

Name (first and last name or first initial and last name)
A person’s previous names used, such as alias names, maiden names, previous married names, or mother’s maiden name

Level 3, Restricted – These data elements are available only to internal authorized users and may be protected by federal and state regulations. Restricted data is intended for use only by individuals who require the information in the course of performing job functions. These are the data elements removed from responses to information requests for reasons of privacy.

Security threats to this data include violation of privacy statues and regulations in addition to unauthorized alteration or destruction. If this data were accessed by unauthorized persons, it could cause financial loss or allow identity theft. Unauthorized disclosure could provide significant gain to a vendor’s competitors.

Examples:
Incident response plans
IP addresses
Firewall hardening standards and configurations
VPN hardening standards
Windows hardening standards
Most home addresses
Competitive bids
Attorneys’ files
Civil investigative data
Comprehensive law enforcement data
Criminal history data
Domestic abuse data
Economic development assistance data
Educational records
Food assistance programs data
Energy assistance programs data
Foster care data
Head Start data
Juvenile delinquent data
Library borrower’s records
Network diagrams
Counselors’ data
Signature imaging data
Trade secrets data
Welfare records/data
Insurance policy number
Passport numbers
Social security numbers
Credit card numbers
Juvenile delinquent data
Driver’s license or state identification card number
Individual’s biometric data, including fingerprints

Bank account number or credit/debit card number, in combination with expiration date, or password that would permit access to financial account

Physical characteristics or description of a person, in combination with first and last name
Any other financial information associated with individuals, vendors, or businesses

Level 4, Critical – Data classified as being critical is data whose disclosure or corruption could be hazardous to life or health. These data elements are the most sensitive to integrity and confidentiality risks. Access is tightly restricted with the most stringent security safeguards at the system as well as the user level. Failure to maintain the integrity and confidentiality could have severe financial, health, or safety repercussions. Very strict rules must be adhered to in the usage of this data.

Security threats to this data include violation of privacy statues and regulations in addition to unauthorized alteration or destruction. If this data were accessed by unauthorized persons, it could have severe financial, health, or safety repercussions.

Examples:
Critical infrastructure information
Protected health information, as covered by the Health Insurance Portability and Accountability Act (HIPAA) that includes any information about health status, provision of health care, or payment for health care that can be linked to an individual