SALT LAKE COUNTY
COUNTYWIDE INFORMATION TECHNOLOGY STANDARD
ON
DATA CLASSIFICATION AND PROTECTION

Purpose-

The purpose of this standard is to emphasize to County agency management and their employees the importance of protecting data generated, accessed, transmitted, and stored by the County and to identify procedures that should be in place to protect the confidentiality, integrity, and availability of County data, and to comply with local and federal regulations regarding privacy and confidentiality of information.

Employees of Salt Lake County are expected to follow the Data Classification and Protection IT Standard established by the Information Technology Division. The Information Technology Division will monitor and enforce compliance with this standard.

Background-

Increased connectivity of computers and databases makes more data available to individuals, businesses, and agencies. As a result, the potential for unauthorized disclosure, modification, or destruction of personal, financial, business, and other data also has increased. There may or may not be laws that regulate the use of a particular data set, and agencies may not be sure how to respond to apparent conflicts between privacy, public records laws, and the need to maintain safety and security. Data classification is a process that identifies what information needs to be protected against unauthorized access, use, or abuse and the extent of that protection.

Reference-

The standards set forth herein are provided in accordance with Countywide Policy 1400, which directs the Salt Lake County Information Technology Division to provide information technology standards. Also referencing the following:

All Countywide Information Technology Security Policies in the 1400 series
All Countywide Human Resource Policies
Salt Lake County Code of Ordinances; Title 2; Chapters 2.81 Security of Personal Identifiers and 2.82 “Records Management.”
All Countywide policies in 1500 series (HIPAA)
All Countywide policies in 2000-2130 series (GRAMA)
Health Insurance Portability and Accountability Act of 1996 (HIPAA); 45 United States Code § 1320d et seq.; Part C Administrative Simplification.
45 Code of Federal Regulations, Parts 160, 162, and 164 (“Privacy Rule”)
Utah’s Government Records Access and Management Act (GRAMA), Utah Code Annotated § 63G-2-102 et seq. (“GRAMA”)

1.0 Scope

All Salt Lake County employees and anyone who uses County information technology resources or systems shall adhere to this Countywide information technology standard.

2.0 Terms and Definitions

County Agency Management

With respect to their own individual offices or departments, any of the following, or their designees: County Mayor, County executive branch department directors, County elected officials, or the County Council (as a whole).

Office of Data and Innovation

The Office of Data and Innovation was created to improve public service by utilizing and sharing data internally and externally, empowering employees to make data-informed decisions, and promoting a culture of continuous improvement.

Technology Advisory Board (TAB)

The Technology Advisory Board (TAB) ensures all information technology initiatives are justified and in alignment with the goals and strategy of Salt Lake County.

GIS Steering Committee

The GIS Steering Committee facilitates cooperation and efficiency within Salt Lake County government by promoting the development, acquisition, and dissemination of GIS infrastructure, data, and services.

County Agency Data Coordinator

Data Coordinators are designated for each agency as the main point of contact and liaison with the Data Governance Working Group on data governance and standards issues.

County Agency Data Custodian

Data Custodians are individuals that assist with the technical implementation of individual databases, datasets, or information systems.

County Data

Data generated, received, transmitted, manipulated, or disposed of by a County agency, irrespective of the medium on which the data resides and regardless of format (such as electronic, paper, or other physical forms).

Data as a Strategic Asset

Data and content of all types are assets with all the characteristics of any other asset. Therefore, they should be managed, secured, and accounted for as other material or financial assets.

Data Catalog

A detailed and comprehensive inventory that makes data appropriately discoverable.

Data Security
Data security means protecting digital data from unauthored access and unwanted actions.

Confidentiality of Data
Maintaining data confidentiality requires ensuring that only authorized users and systems have access to the data.

Data Integrity
Data integrity is the overall accuracy, completeness, relevance, timeliness, and consistency of data and metadata. Maintaining data integrity requires that the data remains correct while in storage or transit and that only authorized changes are made to the data.

Data Accessibility
Data access is the on-demand, authorized ability to retrieve, modify, copy, or move data from IT systems based on organizational roles and responsibilities.

Data Sharing
Data sharing means sending data, receiving data, or advancing shared objectives according to specific terms and conditions.

Data Risk and Liability
Data risk and liability describe the financial liability inherent in all data or content based on regulatory and ethical misuse or mismanagement.

Availability of Data
The concept of availability means authorized users have reliable and timely access to the data and resources they are allowed to use.

Maximum Tolerable Downtime (MTD)
How long a system can be unavailable before it results in a serious situation.

Recovery Point Objective (RPO)
Determines the amount of data you can afford to lose in the event of an outage.

Recovery Time Objective (RTO)
Determines how quickly the system is made available after an outage.

Licensed Data
Licensed data is information made available to County employees and residents only as the result of a subscription or agreement with third-party providers who own, license, and/or aggregate and provide access to this data. According to the terms of subscription licensing agreements, the data must be protected from unauthorized access by anyone except County employees and customers. In addition, this data may be protected by copyright law. Therefore, a reasonable level of control needs to be applied to protect this

intellectual property from theft or reproduction in accordance with the terms of an agreement. The County does not own this data, and if the agreement ceases, access to the data ceases as well.

3.0 Standard Guidance

All Salt Lake County employees and anyone that uses a Salt Lake County IT resource or system will follow the County's Data Security and Protection IT Standard as defined in Appendix A of this document.

4.0 Exceptions

Any exceptions to this standard must be explicitly approved in writing by the Salt Lake County Chief Information Officer or their designee.

5.0 Enforcement

Anyone found to have knowingly violated this IT standard may be subject to disciplinary action in accordance with County disciplinary policies.

Revision History
AUGUST 2021 - MLE

Appendix A
DATA SECURITY AND PROTECTION

Roles and Responsibilities

All County data, regardless of medium or format generated, stored, or received by Salt Lake County and any of its agencies, is the County's property and considered a critical asset of the County. Therefore, county agency management, and staff, shall ensure and are responsible for protecting the confidentiality, integrity, and availability of County data irrespective of the medium on which the data resides and regardless of format. County agencies shall also ensure that Business Associates meet the same data confidentiality, integrity, and availability standards.

Office of Data Innovation

The Office of Data and Innovation was created to improve public service by utilizing and sharing data internally and externally, empowering employees to make data-informed decisions, and promoting a culture of continuous improvement.

County Agency Management

County Agency Management is responsible for ensuring that the appropriate managerial, operational, physical, and technical controls are implemented to access, use, store, transmit, and dispose of County agency data in compliance with this standard. Attestation by County Agency Management on a semi-annual basis will serve as confirmation that County Agency data has been classified properly, that appropriate controls have been implemented, that controls protecting data are adequate, and that County data is secure as required by this standard

Technology Advisory Board

The Technology Advisory Board (TAB) ensures all information technology initiatives are justified and aligned with the goals and strategy of Salt Lake County; initiatives are forward-thinking, cost-effective, add value or benefit, and will be effectively implemented in the best interest of the public. This will be accomplished through working groups appointed by the County Chief Information Officer (CIO), making information technology recommendations to the TAB

GIS Steering Committee

The GIS Steering Committee facilitates cooperation and efficiency within the Salt Lake County government by promoting the development, acquisition, and dissemination of GIS infrastructure, data, and services.

Data Governance Working Group

The Data Governance Working Group works under the Technology Advisory Board (TAB) and GIS Steering Committee to ensure that appropriate mechanisms are in place to establish a culture of operational excellence that recognizes and supports institutional data as an asset of the County.

County Agency Data Coordinator

County Agency Management shall designate a *County Agency Data Coordinator* who will be assigned to work with the Office of Data and Innovation.

- Act as a single point of contact for Data Governance Working Group.
- Serve as a liaison with Data Governance Working Group on issues related to data governance
- Attend training and workshops on data management.
- Assist with system(s) inventory.
- Assist with database(s) inventory.
- Assist with implementing privacy, data licensing, metadata, and other standards and practices.
- Provide feedback regarding data management initiatives to Data Governance Working Group.

County Agency Data Custodian

County Agency Management shall designate a County Agency Designated Data Custodian for each system in current use. The responsibilities of Designated Data Custodians are as follows:

- Implement data protection controls to ensure County agency data is protected.
- Monitor data protection controls to ensure that County agency data is protected.
- Update security controls as the county agency data changes or when better control methods become available.
- Demonstrate compliance with this IT standard to the Office of Data and Innovation upon request. The fulfillment of annual reporting requirements is also to County Agency Management's ongoing duty to protect County agency data.
- Assist with compliance reporting to the Office of Data and Innovation and will attest and confirm that controls are being adhered to and that County data is secure. Attestation will be in the form of their sign-off on the annual reporting documents.

County Information Security Manager

The County Information Security Manager acts as a resource and consultant regarding data security for County agencies.

County Records and Archives Manager

The County Records and Archives Manager serves as a member of the County Data Protection Committee and advises on records retention statutes and policies.

County Risk Manager

The County Risk Manager serves as a member of the County Data Protection Committee and advises on risk management and insurance coverage issues.

Data Security Classification Categories

County Agency Management shall carefully evaluate all County data that they are responsible for and apply the appropriate data classification. County Agency Management will work in association with the County Agency Data Protection Officer, County Agency Designated Data Custodian, and County Data Protection Committee to classify data. All County data must be classified into one of the following three categories:

Public Data
Public data is information that may or must be open to the general public. Public data has no existing local, national, or international legal restrictions on access or usage. While subject to State and County disclosure rules (e.g., GRAMA), public data is available to all individuals and entities. While little or no controls are required to protect the confidentiality of public data, some controls will still be required to prevent unauthorized modification or destruction of public data.

Protected Data
Protected data is information that must be guarded due to legal, proprietary, ethical, or privacy considerations and must be protected from unauthorized access, modification, transmission, storage, or other use. This classification applies even though there may not be a criminal or civil statute requiring this protection. By default, any data that is not explicitly classified as public or restricted should be treated as protected data. Protected data may be disclosed to individuals on a need-to-know basis only or as required by law. A reasonable level of security controls needs to be applied to protected data.

Restricted Data
Restricted data is information protected by federal or state statutes or regulations (e.g., HIPAA), County ordinance (e.g., Ordinance 2.81), contractual language (e.g., PCI-DSS), or licensed data. It must be protected from unauthorized access, modification, transmission, storage, or other use. Restricted data shall be disclosed where required by applicable law. Restricted data warrant the highest security controls within the organization unless a lesser level of security controls are required for a specific data set.

Disaster Recovery/Continuity of Business Classification Categories
Tier-1
Maximum Tolerable Downtime (MTD) - Less than 24-hours
Recovery Point Objective (RPO) - Less than 1-hour
Recovery Time Objective (RTO) - Less than 24-hours

Tier 2
Maximum Tolerable Downtime (MTD) - Less than 1-day
Recovery Point Objective (RPO) - Less than 1-hour
Recovery Time Objective (RTO) - Less than 24-hours

Tier 3
Maximum Tolerable Downtime (MTD) - Less than 7-days
Recovery Point Objective (RPO) - Less than 24-hours
Recovery Time Objective RTO) - Less than 1-week

Tier 4
Maximum Tolerable Downtime (MTD) - Less than 1-month
Recovery Point Objective (RPO) - Less than 24-hours
Recovery Time Objective (RTO) - Less than 1-month