SUBJECT: DATA GOVERNANCE AND PROTECTION POLICY

I. **INTRODUCTION**: Data governance is a shared system by which data is managed. Institutional data is viewed as a key asset and shall be protected by applicable institutional, state and federal guidelines from deliberate, unintentional, or unauthorized alteration, destruction or disclosure. Institutional data will be identified, defined, and controls will be put in place to manage data completeness, data validity and reduce data redundancy. Data will be made accessible based on an employee's need and their University role. Institutional representatives will be held accountable for performing their data management responsibilities. As outlined in SUU *Policy 5.57, Information Technology Resource Security*, contingency plans for data backup, disaster recovery and incident response will be implemented and maintained. This policy identifies the University's: (a) data types, (b) data ownership, (c) data governance structure, and (d) employee data protection responsibilities.

II. **REFERENCES:**

A. SUU Policy and Procedures, *5.57 Information Security Resources*

B. SUU Policy and Procedures, *5.51, Information Technology Resources*

C. SUU Policy *5.52, Intellectual Property*

D. SUU Policy and Procedures, *6.22, Faculty Due Process*

E. SUU Policy and Procedures, *8.3.5, Termination of Non-Academic Staff Employees and Disciplinary Sanctions*

F. SUU Incident Response Plan

G. SUU Private Personal Information Data Protection Agreement

H. SUU Private Personal Information Authorization Form

I. Acknowledgements: USHE Information Technology Resource Security Policy (Policy R345)

J. Acknowledgements: Utah Code, Title 63G, Chapter 2, Government Records Access and Management Act (GRAMA)

K. Acknowledgements: Family Educational Rights and Privacy Act (FERPA)

L. Acknowledgements: Health Insurance Portability and Accountability Act (HIPAA)

M. Acknowledgements: Columbia University Electronic Information Resources Security Policy

N. Acknowledgements: Stanford University Data Governance and Stewardship

III. **PURPOSE**: To establish approved policy for the proper access, handling, and protection of personal information of Southern Utah University (SUU) students, employees and constituents. The overarching goal of the policy is to have University data protected against unauthorized access and use.

IV. **SCOPE**: This policy applies to all SUU constituents, including faculty, staff, students, student workers, contract employees, temporary employees, consultants, contractors, vendors, and third-party agents of the University. This policy covers all categories of data regardless of what format the data is stored or transmitted (physical or electronic). Said policy covers all data that is collected for business purposes and stored on University-owned administrative and networking systems. Data collected for research purposes is covered under SUU Policy *5.52, Intellectual Property*.

V. **DEFINITIONS**:

A. Acceptable Information Technology Usage Guidelines: The University's acceptable usage guidelines are outlined in *SUU Policy 5.51, Information Technology Resources*.

B. Administrative and Networking Systems: Technology that includes, but is not limited to: (a) computers, (b) laptops, (c) servers, (d) phones, (e) storage systems, and (f) other portable devices.

C. Credit Card Security Codes (CAV2/CVC2/CVV2/CID): Credit card security codes are the 3- or 4-digit codes on the back of a credit card.

D. Data Access: The right to read, copy or query data.

E. Data Council: SUU's Data Council is composed of the University's Data Stewards and operates in an advisory role, focusing on six areas: (a) data policies and standards, (b) data quality, (c) data architecture, (d) privacy compliance, (e) establishing standardized, transparent and documented processes and (f) data

conflict resolution regarding data attributes and level of access.

F. Data Managers: Data Managers oversee the administrative and networking systems where data reside. This includes, but is not limited to: (a) computers, (b) laptops, (c) servers, (d) phones, (e) storage systems, and (f) other portable devices.

G. Data Stewards: Data stewards are business process owners. Stewards: (a) identify the data they are responsible for, (b) create standards and controls for said data, and (c) create environments where the data under their purview is used properly. Data Stewards are the administrators responsible for functional operations that handle institutional information processing. Said areas include, but are not limited to the following offices: (a) Registrar's, (b) Financial Aid, (c) Admissions, (d) Human Resources, (e) Development, (f) Controller's, and (g) Student Affairs.

H. Data Types: All institutional data falls into one of three data types: (a) public, (b) protected, or (c) private.

I. Data Users: Data Users are employees or agents of the University who access University data as part of their daily assigned duties. Access may include reading, entering or downloading data.

J. Device: Any type of computing, display, or application-based device, including, but not limited to, desktop computers, laptops, tablets, smartphones, etc. A device also includes removable media such as flash drives, CDs, DVDs, external/portable hard drives, etc.

K. Encryption: The conversion of data so that said data is not easily understood by unauthorized users.

L. Family Educational Rights and Privacy Act (FERPA): A federal law that protects the privacy of student education records.

M. Health Insurance Portability and Accountability Act (HIPAA): A federal law that protects the confidentiality and security of protected health data when it is transferred, received, handled, or shared.

N. Incident Response Plan: An organized strategy for dealing with the consequences of a security event (physical or electronic). The purpose of the plan is to mitigate damage and reduce recovery time.

SUBJECT: DATA GOVERNANCE AND PROTECTION POLICY

O. Information Technology Resource Security Guidelines: The University's guidelines regarding information security are located in SUU *Policy 5.57, Information Technology Resource Security.*

P. Institutional Data: Data is a compilation of facts collected for future use and may or may not be used to make future University decisions and include data element(s) that are relevant to the planning, management, operating, or auditing functions of the University. Institutional data is created, received, maintained, or transmitted as a result of educational/research purposes.

Q. Payment Card Industry (PCI): PCI is a set of security standards that were developed to protect card information during and after a financial transaction.

R. Personal Identification Number (PIN): A PIN is a numerical code used in many electronic financial transactions. PINs are usually used in conjunction with usernames or other passwords.

S. Personally Identifiable Information (PII): Data that can be used to identify a specific person or entity. Includes items such as name, address, phone number, birth date, bank or other account number, credit or debit card number, social security number, medical history information, etc. Personal Information is classified by three data types: (a) Public Data, (b) Protected Data, and (c) Private Data.

T. PIN Block: A PIN block is a block of data that encapsulates a PIN during processing.

U. Public Data: Information with no existing local, state, national, or international legal restrictions on access or usage. Public data poses little to no risk to the University's services or stakeholders.

V. Private Data: Information protected by statutes, regulations, University policies, or contractual language. Private Data may be disclosed to individuals on a need-to-know basis.

W. Protected Data: Information that must be guarded due to 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 civil statute requiring this protection and is restricted to

members of the University community who have a legitimate purpose for accessing such data.

X. University Funds: All funds, regardless of the source, which are owned, held, or administered by the University including state appropriations, tuition, federal appropriations, generated income, student funds, auxiliary and agency funds, or funds from gifts, grants, and contracts.

Y. University Property: All equipment, devices, services, data, etc. donated to the University or purchased with University Funds as defined above.

VI. PRINCIPLES:

The following principles are identified as minimum standards that govern the usage of University data:

A. Institutional data shall be protected according to University, USHE Regents, federal, and Utah state guidelines/regulations as well as applicable regulations from other jurisdictions and industries (e.g., GDPR, PCI). Any future changes to the aforementioned regulations that contradict or enhance any part of this policy shall take precedence.

B. Institutional data standards will be defined and utilized.

C. Institutional data will be monitored.

D. Institutional data will be accessible based on defined need and user role.

E. Unnecessary data duplication is prohibited.

F. Unnecessary updating of data is prohibited.

G. Data Users will be held accountable for their data roles and responsibilities.

H. Resolution of data issues will follow consistent processes outlined by the Data Council.

VII. POLICY:

A. **Data Ownership:** While specific units are responsible for maintaining certain

datasets, no one person or entity owns University data. Data ownership resides with the institution as a whole.

B. **Data Types:** In the process of conducting daily business, SUU collects many different types of data, including but not limited to: (a) academic, (b) research, (c) financial, (d) human resources, (e) alumni, (f) facilities, (g) library, (h) student, (i) clinical, (j) development, and (k) other personal data sources. With this collection comes the onus to maintain and protect said data.

1. **Public Data:** Public data is information that may or must be open to the general public. It is defined as information with no existing local, national, or international legal restrictions on access or usage. Public data, while subject to University disclosure rules, is available to all members of the University community and to all individuals and entities external to the University community. Examples of public data include, but are not limited to: (a) names, (b) addresses, (c) phone numbers, (d) campus maps, (e) campus events, (f) course descriptions, (g) press releases, and (h) research publications. Due to its nature as being generally available to and accessible by the public, Public Data may be accessed and used by any University employee. Public Data does not require encryption and may be processed, accessed, and transmitted via any method (electronic, paper, etc.) or via any device, including mobile devices.

2. **Protected Data:** Protected Data is information that must be guarded due to 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 civil statute requiring this protection. Protected Data is information that is restricted to members of the University community who have a legitimate purpose for accessing such data. By way of illustration only, some examples of Protected Data include, but are not limited to: (a) donor contact information and non-public gift amounts, (b) birth dates, (c) University T Numbers, (d) student grades and other academic performance information, and (e) last four (4) digits of an individual's social security number and full name in combination with mother's maiden name or date of birth.

   Protected Data access and use is limited to members of the University Community and authorized third parties via contractual agreements who have a legitimate business purpose to access the data. Sufficient due care

concerning proprietary, ethical, or privacy considerations should be exercised when handling and/or transmitting Protected Data. Protected Data accessed outside of the University network shall be accessed through secure channels, such as the University's Virtual Private Network (VPN) system and should only be stored in secure locations. Encryption of Protected Data is recommended, but is not required.

3. **Private Data:** Private Data is information protected by statutes, regulations, University policies, or contractual language. Private Data access and use is limited to members of the University Community and authorized third parties via contractual agreements who have a legitimate business purpose to access the data. Southern Utah University defines Private Data in the forms of Private Personal Information, Protected Health Information and Payment Card Industry Data. Examples of Private Data include but are not limited to: (a) full social security numbers, (b) bank account and/or investment account numbers, (c) driver's license or state identification numbers, (d) passport or visa numbers, (e) alien registration numbers, and (f) account usernames in conjunction with passwords and/or other security access codes or phrases that would permit access to individuals' accounts.

   Examples of private protected health information (federally protected under HIPPA) include, but are not limited to: (a) biometric identifiers such as fingerprints, voice prints, etc.; (b) medical record or medical account numbers; (c) patient notes; (d) diagnosis or ICD codes; (e) treatment or CPT codes; (f) account usernames in conjunction with passwords or other security access codes/phrases that would permit access to an individual's personal health information; (g) any unique identifiers used by a health care professional or health insurer to identify an individual; and (h) any other information regarding an individual's medical history, mental or physical condition, or medical treatment/diagnosis by a health care professional.

   Examples of private PCI data include, but are not limited to: (a) primary account numbers (PAN), (b) cardholder names accompanied by PAN, (c) service codes, (d) expiration dates, (e) full magnetic stripe data, (f) card security codes (CAV2/CVC2/CVV2/CID), and (g) PIN/PIN Block.

   Private Data comes with access and usage requirements:

SUBJECT: DATA GOVERNANCE AND PROTECTION POLICY

a. **Authorization:** Only authorized users shall have physical/hard copy, electronic, or other access to Private Data. Authorization must be obtained in writing or electronically from the President or authorized designee via SUU's Authorization to Access Private Data form. Said forms shall be reviewed, updated, and approved periodically, at least annually. Private Data should not be accessed, viewed, downloaded, input, copied, scanned, or otherwise obtained without prior written or electronic authorization. Each employee that has access to Private Data must also sign the Private Personal Information Data Protection Agreement.

b. **Access:** Private Data in electronic form must be encrypted and can only be accessed via University issued and approved devices. Private Data in physical/hard copy form may only be viewed by authorized users. Private Data is not to be accessed or stored on any personal equipment or device, including but not limited to, home computers and/or laptops, personal tablets or smartphones, or any other type of personal device whether mobile or stationary. Only secure methods may be used to access, input, store, or transfer Private Data on any device. All off-campus access gained to Private Data must be through secure channels, such as the University's VPN system. Private Data must only be transmitted or shared via secure methods or channels as approved by the Information Security Office.

c. **Storage:** Private Data in the custody or control of SUU employees should be stored only when there is a legitimate academic or business necessity. Electronically stored Private Data must be encrypted and stored in University approved locations determined by the Information Security Office. Exceptions to encryption are only allowed as noted in the Exceptions section below. Cloud services such as Dropbox, Google Drive, iCloud, or any other similar program or systems must not be used with any files or data containing Private Data until the Information Security Office determines that data stored and transmitted to/from cloud-based services can be encrypted or otherwise sufficiently secured and protected. Private Data in physical /hard copy form should be stored in secure locations to which only employees authorized to view Private Data have access. Private Data shall never be stored

on removable media such as: (a) flash drives, (b) CDs, (c) DVDs, or (d) external portable hard drives.

d. **Private Data Destruction:** Private Data in all forms (hard copy, electronic, etc.) should be properly and adequately deleted and/or destroyed from all files and devices as soon as the academic or business need is fulfilled. Electronic Private Data must be securely wiped using approved data destruction software. Private Data in physical/hard copy form must be cross cut shredded.

e. **Exceptions:** Any exceptions must be obtained from the Information Security Office in writing or electronically.

f. **Private Data Protection and Management:**

i. Equipment, devices, files, etc. purchased with University funds or donated to SUU are the property of the University. The University reserves all rights to scan, inspect, review, etc. all University-owned equipment, devices, and files at any time and take any necessary action to ensure the protection of any Private Data found thereon. Users should be aware that their uses of University Information Technology Resources are not private (SUU *Policy 5.51*).

ii. In order to ensure adequate protection of Private Data, the University may, at its discretion, use software programs or other methods to identify where Private Data is located and/or stored electronically or in physical form and monitor its use and protection. This includes the installation of data identification and data protection software on University-issued devices, as well as the option to centrally push out scans of equipment and devices connected to the University's network.

C. DATA GOVERNANCE STRUCTURE:

1. The following roles and responsibilities are established to delineate clear governance accountability over institutional data.

SUBJECT: DATA GOVERNANCE AND PROTECTION POLICY

a. **President's Cabinet:** The President's Cabinet is the administrative body that leads the University. Each Presidential Cabinet Representative is responsible for overseeing Data Governance and Protection for the University and their respective areas.

b. **Chief Information Officer (CIO):** The CIO is responsible for setting and enforcing IT standards.

c. **Director of Administrative Systems:** The Director of Administrative Systems is responsible for all enterprise application operations and support to the students, faculty, staff and administration of the University. This includes: (a) application development, (b) enterprise system administration and deployment, (c) related project management and coordinating support to the departments and individuals that depend on central administrative applications.

d. **Director of IT Security:** The Director of IT Security is responsible for overseeing data security for the University, to include implementing and enforcing policies, procedures, and guidelines. This includes routine activities such as (a) analyzing network traffic, (b) reviewing logs, (c) documenting security events, (d) training users, (e) recommending, implementing, and assessing security controls, and (f) adhering to best practices of the computer security industry.

e. **Data Council:** The Council is composed of the University's Data Stewards (representatives from each major data management area) and operates in an advisory role. The Data Council focuses on six areas: (a) data policies and standards, (b) data quality, (c) data architecture, (d) privacy compliance, (e) establishing standardized, transparent and documented processes, and (f) data conflict resolution regarding data attributes and level of access.

f. **IT Governance Committee:** The IT Governance Committee coordinates key issues that affect IT across the institution. The main purpose of the Committee is to align the University's technology resources with its mission and strategic plan priorities.

g. **Risk Management Committee:** The Risk Management Committee identifies, evaluates and manages entity-wide risk in order to provide a safe environment for the campus community. This includes the development of safety and risk programs which include, but are not limited to: (a) environmental compliance, (b) occupational safety and health, (c) IT security, and (d) property and liability insurance.

i. **PCI Committee:** The PCI Committee is a subcommittee of the Risk Management Committee and maintains/promotes PCI standards for the safety of cardholder data across the campus. Said Committee is charged with meeting current PCI security standards while keeping the institution's systems secure, thereby protecting sensitive payment card information.

h. **Data Stewards:** Data Stewards are business process owners. Stewards: (a) identify the data they are responsible for, (b) create standards and controls for said data, and (c) create environments where the data under their purview is used properly. Data Stewards are the administrators responsible for functional operations that handle institutional information processing. Said areas include but are not limited to the following offices: (a) Registrar's, (b) Financial Aid, (c) Admissions, (d) Human Resources, (e) Development, (f) Accounting Services, and (g) Student Affairs.

Data Stewards responsibilities include: (a) ensuring that all applicable University, state and federal regulations are adhered to; (b) classifying each data element as Public (low risk), Protected (medium risk,) and Private (high risk); (c) defining the procedures for employee access to data; (d) outlining procedures for internal and external constituents to request University data; (e) resolving issues involving data definitions, data policy and levels of data access; (f) approving data access for functions under their purview; (g) providing initial data documentation and future updates for all data elements (source and definition) from their respective areas; (h) collecting only information that is needed for legitimate University purposes; (i) coordinating with the Data Council prior to making any data changes, (j) creating proper protocol regarding

data manipulation, extracting and reporting; (k) ensuring that all administrative and networking systems that reside under their purview have received the latest patches/security updates, (l) understanding and complying with data access and privacy principles (FERPA, HIPPA, etc.); (m) storing data in appropriate storage locations as defined by the Information Security Office; (n) ensuring data integrity/accuracy through the data's life cycle; (o) maintaining data based on the UT Retention Schedule and developing a data purge process for data that is no longer needed for business purposes; (p) providing data training for all data users in data entry, handling, security, and retention; (q) collaborating with other Data Stewards to maximize enterprise operations; (r) ensuring that data requestors are authorized to receive said information; (s) using data only for specified purposes; (t) coordinating with the Director of IT Security regarding best practices; (u) reporting any data breaches; and (v) taking appropriate action for data violations, including but not limited to administering employee disciplinary actions.

i. **Data Managers**: Data Managers oversee the administrative and networking systems where data reside. This includes, but is not limited to: (a) computers, (b) laptops, (c) servers, (d) phones, (e) storage systems, and (f) other portable devices. Data Managers are responsible for maintaining and securing the data that is generated in the various Data Steward areas.

Data Manager responsibilities include: (a) ensuring that all applicable University, state and federal regulations are adhered to; (b) encrypting data where required; (c) informing Data Users of where to store, backup and retrieve information; (d) coordinating technical support for Data Users; (e) recommending appropriate information security requirements and training the campus community on said requirements; (f) installing and using a Protected Data monitor such as Identity Finder to accurately identify and classify business critical, regulated and protected University data; (g) continually monitoring network events; (h) defining data mitigation and recovery procedures, (i) with feedback from Data Stewards, documenting each data element (source, name, definition), (j) educating Data Stewards and Users

regarding secure handling and management of data; and (k) reporting any data breaches.

j. **Data Users**: Data Users are employees or agents of the University who access University data as part of their daily assigned duties. Access may include reading, entering or downloading data.

Data User responsibilities include: (a) ensuring that all applicable University, state and federal regulations are adhered to regarding data access, use, security, disposal, and disclosure; (b) protecting the privacy and confidentiality of the records they access; (c) refraining from unnecessary data duplication or data updates; (d) accessing only the data that is required for the position; (e) storing information under secure and appropriate conditions; and (f) reporting any data breaches.

D. **Training and Certification:** Data security training and certification will be governed by the Information Security Office, the Data Council and University Administration.

E. **Violations:** Violations of this policy constitute sufficient cause for termination. University personnel who violate this policy will be subject to the sanctions and remedies described in: (a) SUU *Policy 5.57, Information Technology Resource Security*; (b) *SUU Policy 8.3.5, Termination of Non-Academic Staff Employees and Disciplinary Sanctions;* and (c) SUU *Policy 6.22, Faculty Due Process*. University personnel may additionally be held personally responsible to the extent allowable under law for any losses or damages caused by their negligence or willful violation of this Data Governance and Protection Policy.