Preamble. Data and information are important assets of the university and must be protected from loss of integrity, confidentiality, or availability in compliance with university policy and standards, Board of Regents policy, applicable contracts, and state and federal laws and regulations. This sets forth the responsibility of users to classify and apply appropriate protections for university data and the systems on which store or process data.

A. Definitions.

A-1. Data Owner: The senior university college/division/departmental executive with direct responsibility for all access and use of designated types of data. Use of this term, in connection with this policy shall not affect university claims or rights of ownership of data or ownership of third party data in the possession of the university. For example, research data produced by the university is owned by the university under current policy, FSH 5700, but the Vice President for Research and Economic Development would be considered the Data Owner for the terms of this policy, APM 30.11.

A-2. Data Steward: The documented employee with expertise in a data area, who is responsible to the Data Owner to ensure appropriate access controls and protections are applied to maintain compliance. The Data Steward coordinates with the Data Owner and University’s Information Security Office on data categorization and determining proper responses to security incidents involving the data with which they are entrusted.

A-3. Operator: Any individual tasked with handling or processing data for the university. This includes contracted vendors or affiliates accessing university data resources on behalf of the Data Owner.

A-4. Data Security Standards: The minimum set of technical and administrative controls required to protect a category of data and meet the objectives of confidentiality, integrity and availability. Supplemental requirements may be published by ITS in cooperation with Data Owners, or defined by other university policies to meet security objectives including compliance requirements.

A-5. System: A discrete set of resources assembled to store, process, maintain, share, or dispose of data. This includes, but is not limited to, any endpoint devices (desktops, laptops, smart phones, tablets) as well as servers, networks, or third party and cloud services.

B. Policy.

B-1. General. Data and information systems must be classified according to the risks associated with data being stored, accessed, or processed. Data with the highest risk needs the greatest level of protection; data with lower risk requires proportionately less protection. Consistent with Federal Information Processing Standards (FIPS) Publication 199, university data is classified based on the impact to individuals or the university if the security of that data was
breached. Data Owners may designate a higher general risk level for a particular data set or establish supplemental standards to the baseline for the risk category.

**B-2. Categories.**

(a) Low Risk. The potential effect of loss of confidentiality, integrity, or availability could be expected to have only a limited adverse effect on the university operations, individuals, or assets. Example: published public information including press releases, directory information, or research data not otherwise confidential or regulated.

(b) Moderate Risk. The potential effect of loss of confidentiality, integrity, or availability could be expected to have a serious adverse effect on university operations, individuals, or assets. Example: FERPA

(c) High Risk. The potential effect on loss of confidentiality, integrity, or availability could be expected to have a severe or catastrophic adverse effect on university operations, individuals, or assets. Example: private information that must be protected by law or industry regulation (HIPAA ePHI, Social Security Numbers, driver’s license numbers, bank or credit account numbers).

**B-3. Data Security Standards.** Data, accounts, and systems must be classified according to the highest risk data that they process. All users and systems accessing university technology resources must meet or exceed required standards based upon the highest data classification stored or accessed by that system. The ITS Information Security Office shall publish, and at least annually review, data security standards with appropriate advisory groups and approved by the Chief Information Officer (CIO).

(a) Published standards shall include, but not be limited to:
(1) Minimum Security Standards (formerly Network Computing Device Standards) which must be met for all systems utilizing the university network or processing data on behalf of the university and classified as low risk.
(2) Moderate Risk Standards which must be met for all systems categorized as moderate risk.
(3) High Risk Standards which must be met for all systems categorized as high risk.
(4) Supplemental standards or references required to meet compliance, contractual, or other policy or industry regulation requirements (e.g., current Payment Card Industry Data Security Standards (PCI-DSS)).
(5) Requirements as outlined in the National Institute of Standards and Technology (NIST) Special Publication 800-171, or its current revision.

(b) Unless otherwise specified or required, changes to published standards shall be effective 90 days from date of publication after approval by the CIO. Where possible, additional notice will be given for significant changes to standards.

**B-4. Compliance.** Systems or users known to be out of compliance with this policy and published standards will be subject to removal of access from university technology resources or data. Where appropriate, ITS will inform the proper internal authority, including the Data Steward, Office of Risk
Management, or Office of Research Assurances, as applicable, of the non-compliance. The applicable internal authority will initiate disciplinary action for non-compliance, where appropriate.

B-5. Reporting Incidents. In the event of a suspected incident or event, including non-compliance with this policy involving any university technology resources which has the potential to adversely affect the university, immediate notification of the incident must be sent to the following:

- ITS Security Office (security@uidaho.edu)
- The Data Steward (if known)

After the incident has been reported, it shall be investigated and escalated in accordance with the university’s Technology Security Incident Response Plan.

C. Scope. This policy applies to all university faculty, staff, students, and affiliates accessing, storing, and processing university data or using university systems or technology resources.

D. Exceptions. Requests for exceptions in all or part of this policy may be submitted in writing to the Information Security Officer who will assess the risk and make a recommendation to the appropriate Data Steward and/or the Chief Information Officer for review or possible approval. Any exceptions must be reviewed at least annually.

E. Contact Information. The ITS Information Security Office (its-security@uidaho.edu) can assist with questions regarding this policy and related standards.

F. References.

- FIPS Publication 199
- NIST SP800-171
- NIST SP800-53rev.4
- UI - FSH 5300 - Copyrights, Protectable Discoveries and Other Intellectual Property Rights
- UI - FSH 5700 – Research Data
- UI - APM 45.19 - Export Controls, U.S.
- UI - APM 45.22 – Eligibility, Competency and Effort Requirements for Principal Investigators, Co-Principal Investigators, and/or Project Directors
- UI – APM 65.02 and 65.06