Policy # 227
Former # 12.4
Date Approved:
Date Amended: 1-18-2019
Responsible Office: Information Security

SUBJECT: INFORMATION SECURITY POLICY

1.0 SUMMARY

1.1. The Snow College Information Security Policy ("Policy") applies to all organizations within the College, although the data needed and used by those organizations are different. Additionally, all College owned devices including, but not limited to workstations, lab computers, and kiosks are affected by this Policy unless otherwise stated. **The principles of academic freedom and free exchange of ideas apply to this Policy, which is not intended to limit or restrict those principles.** This policy is intended to be in accordance with federal and state laws and regulations regarding information security.

1.2. Each organization within the College must appropriately apply this policy to make certain they are meeting the requirements regarding Information Security. It is recognized that the technology at some organizations may limit immediate compliance with the policy; such instances of non-compliance must be reviewed and approved by the Information Security Office (ISO) and the Information Security Advisory Council (ISAC). Reference Section 4.19 for more information about policy exceptions.

1.3. College information technology resources are a valuable college asset and must be managed accordingly to assure their integrity, security, and availability for lawful educational purposes. This document describes the policy for use by all persons and/or organizations that have access to College data.

1.4. Readers should note that the appendices of this policy and any referenced standards are enforceable as part of the policy and are subject to change.

1.5. Note: Throughout the policy the terms data and information are used interchangeably.

1.6. Note: This policy applies to mobile devices as applicable. For additional requirements pertaining to tablets and smartphones see Mobile Device Policy (**12.5**).

2.0 PURPOSE

2.1. Provide policy to secure Personally Identifiable Information (PII) of College employees, students, and others affiliated with the College, and to prevent the loss of information that is critical to the operation of the College.

2.2. Provide reasonable and appropriate procedures to assure the confidentiality, integrity, and availability of the College's information technology resources.

2.3. Prescribe mechanisms which help identify and prevent the compromise of information security and the misuse of College data, applications, networks, and computer systems.

2.4. Define mechanisms which protect the reputation of the College and allow the College to satisfy its legal and ethical responsibilities with regard to its networks' and computer systems' connectivity to networks outside the College.

2.5. Provide written guidelines and procedures to manage and control information considered to be PII whether in electronic, paper, or other forms.

2.6. Protect the integrity and validity of College data.

2.7. Assure the security and protection of PII in the College's custody, whether in electronic, paper, or other forms.

3.0 DEFINITIONS

3.1. *Centralized Computer Systems* - Computer hardware (including but not limited to servers, routers, switches, and access points) and software systems (including but not limited to Web hosts, customized databases, College databases, and faculty developed software for educational purposes) maintained by the IT Division and located in areas managed by IT personnel.

3.2. *Computing Equipment* - All hardware used to process, store, or transmit College data.

3.3. *Data* - Information contained in either College computer systems or in physical copy that is utilized for the purposes of conducting College business or learning.

3.4. *Decentralized Computer Systems* - Computer hardware (including but not limited to servers, routers, switches, and access points) and software systems (including but not limited to Web hosts, customized databases, College databases, and faculty developed software for educational purposes) maintained by any non - IT Division department.

3.5. *Information Technology Resource (IT Resource)* - A resource used for electronic storage, processing or transmitting of any data or information, as well as the data or information itself. This definition includes but is not limited to electronic mail, voice mail, local databases, externally accessed databases, CD-ROM, recorded magnetic media, photographs, digitized information, or microfilm. This also includes any wire, radio,

electromagnetic, photo optical, photo electronic or other facility used in transmitting electronic communications, and any computer facilities or related electronic equipment that electronically stores such communications.

3.6. *Kiosk* - Computers located in public spaces designed to offer limited functionality with specialized hardware or software.

3.7. *Lab* - A collection of computers that are either available for general use or are in a secured academic environment that are intended for specific use by students, faculty or staff.

3.8. *Mobile Device* - Any handheld or portable computing device including running and operating system optimized or designed for mobile computer, such as Android, Apple's iOS, or Windows Mobile. Any device running a full desktop version operating system is not included in this definition.

3.9. *Portable Equipment* - Laptops and other removable storage devices such as flash drives.

3.10. *Public Information* - Information that may be provided openly to the public.

3.11. *Security* - Measures taken to reduce the risk of (a) unauthorized access to IT resources via logical, physical, managerial, or social engineering means; and/or (b) damage to or loss of IT resources through any type of disaster, including cases where a violation of security or a disaster occurs despite preventative measures.

3.12. *Personally Identifiable Information: (PII)* Any data, electronic or physical copy, of which the compromise with respect to confidentiality, integrity, and/or availability could have a material adverse effect on Snow College interests, the conduct of College programs or the privacy to which individuals are entitled. Examples of such data would include that data protected by the Government Records Access and Management Act (GRAMA), Family Education Rights and Privacy Act (FERPA), Gramm-Leach-Bliley Act (GLBA) or other laws governing the use of data or data that has been deemed by the College as requiring protective measures. Also included in this class of information are credit card and Social Security numbers. (For additional information on data classification types, reference policy 12.2 Data Classification and Handling.)

3.13. *Strong Password* - A password that is at least 8 characters long and is a combination of upper and lower case letters, numbers and special characters. Strong passwords do not include commonly used phrases, names, or other types of dictionary words.

3.14. *User* - All persons and/or organizations that have access to College data.

3.15. *Workstation* - Computers assigned to one or more College employees for conduction College business.

4.0 POLICY

Information security or protection of confidential personal and internal information departments and other College units must take measures to protect PII and internal information that is used, processed, transmitted, or stored on IT resources in accordance with this policy and any additional information security rules developed by data stewards and/or ISO.

4.1. *Information Confidentiality and Privacy*. All users are expected to respect the confidentiality and privacy of individuals whose records they access. Users are responsible for maintaining the confidentiality of data they access or use and the consequences of any breach of confidentiality.

4.2. *Handling Sensitive/Restricted Information*. The unauthorized addition, modification, deletion, or disclosure of PII included in College data files is expressly forbidden.

4.3. *Centralized/Decentralized Computing Systems*. All computing systems will be in compliance with this policy and College Security standards regardless of whether they are centralized or decentralized. Any decentralized computing systems that are unable to comply with the requirements of this policy may be required to relocate to the College Data Center at the discretion of the ISAC and ISO.

4.4. *Personally Identifiable Information Collection*. PII must only be collected for lawful and legitimate College purposes according to the requirements outlined in Utah System of Higher Education (USHE) Policy R345 – Information Technology Resource Security.

4.5. *Public Information*. Although there are no restrictions on disclosure of public information, the same precautions prescribed in this policy for protection of College data must be adhered to for the purpose of preventing unauthorized modification, deletion, etc. of public information.

4.6. *Access Control*. Access to College data and its resident computing system will be restricted to those users that have a legitimate business or educational need and appropriate approvals for access to such information. Users must ensure that PII is secured from unauthorized access and are responsible for safeguarding this information and related computing systems at all times through the use of strong passwords and as outlined in the Access Control Section of Appendix B.

4.7. *Remote Access*. Only authorized users will be permitted to remotely connect to College computer systems, networks and data repositories to conduct

College related business as required by the standard for secure remote access.

4.8. *Physical Security*. The physical security of computing resources will be accomplished utilizing current industry standards and appropriate technology and plans as defined by the ISO. Responsibility for centralized computing systems security will reside with the IT office. All other computing systems security will be the responsibility of the appropriate IT office specialist. See the Physical Security section of Appendix B for specific requirements.

4.9. *Data Security.* Users will ensure PII is secure and the integrity of records is safeguarded in storage and transmission. Users who handle PII are responsible for the proper handling of this data while under their control. Refer to the Data Security section of Appendix B for specific Data Security Requirements.

4.10. *Backup and Recovery*. Administrators of centralized computing systems will backup essential College data according to a documented disaster recovery plan consistent with industry standards and store such data at a secure commercial site. Decentralized computing systems will have available, at a minimum, a documented disaster recovery plan covering backup procedures, timelines, storage locations/procedures, and recovery.

4.11. *Security Incident Response and Handling*. All suspected or actual security breaches of College or departmental system(s) will be reported immediately to the organization's data security steward who will consult with the ISO to assess the level of threat and/or liability posed to the College or affected individuals and respond according to incident response guidelines maintained by the ISO. The College will report and/or publicize unauthorized information disclosures as required by law or specific industry requirements.

4.12. *Service Providers*. Service providers utilized to design, implement, and service technologies must provide contractual assurance that they will protect the College's PII it receives according to College or commercially reasonable standards. Such contracts must be reviewed by College Legal Counsel for appropriate terminology regarding use and protection of PII.

4.13. *Training and Awareness*. Each new College employee will be trained on the IT Technology Acceptable Use Policy and College Information Security Policy as they relate to individual job responsibilities. Such training will include information regarding controls and procedures to prevent employees from providing data to an unauthorized individual. All employees will be required to complete additional security training as prescribed by the ISO.

4.14. *Computer Labs*. Snow College provides robust computing lab resources for utilization in legitimate and lawful academic endeavors. Computing equipment in these labs will conform to all requirements of this policy with the addition of requirements stated in the Computing Lab Section of Appendix B.

4.15. *Software.* Only properly licensed software may be installed on College computer systems.

4.16. *Penalties and Enforcement*. Penalties and enforcement of this policy will be in accordance with College policies. Appropriate disciplinary and/or legal action will be taken when warranted in any area involving violations of this policy.

4.17. *Policy Review and Revision*. This policy and its associated appendices will be subject to periodic review and revision.

4.18. *Policy Clarification*. For clarification or further information on any items in this policy, the user is encouraged to contact the ISO, their data security steward or a member of the ISAC.

4.19. *Exceptions to Policy*. Any computing system that is unable to comply with this policy must file an exception. Exceptions to this policy must be approved by the ISO based on academic or business need and reviewed by the ISAC. The ISO will review exceptions annually for continued application and notify the exception holder of any concerns.

4.20. *Additional Policies.* Users should be aware that there are additional policies from other governing bodies that affect information security on campus and are outside of the College's Policy and Procedures Manual. Users should be familiar with the policies listed below and ensure their security practices are in adherence to these policies at all times.

4.20.1. Board of Regents (BOR) R345 - Information Technology Resource Security

5.0 SCOPE

5.1. This policy covers paper-based and electronic data defined to include, but not be limited to, all information maintained, processed, or distributed by the College computer systems that contain data defined by law or policy as PII. This policy also applies to all persons and organizations that have access to College data.

APPENDIX A: ROLES AND RESPONSIBILITIES

The persons responsible for implementing this policy and their respective duties and/or responsibilities with respect to this policy are described here.

College Deans/Managers/Supervisors - These individuals shall be responsible for oversight of their employees' authorized use and access to College data in their areas of supervision. They will:

- Ensure that the management and control of risks outlined in this policy are adhered to by employees in their unit.
- Ensure employees' access to College data is appropriate.
- Regularly review and document employee access to College data.
- Identify the necessary Data Security Steward and ensure they receive adequate training to perform this role.
- Provide employees with resources and methods to properly secure equipment where College data is processed, stored, or handled.
- Provide employees with approved resources and methods for external data storage where College data is processed, stored, or handled.

IT Specialist - These individuals are responsible for being the technical support within a business unit, college/school, or department.

Data Security Steward - These individuals are responsible for business processes within their areas of supervision will:

- Understand current information security policies, standards and guidelines and act as a point of contact for questions regarding information security and direct the user to the appropriate source (e.g., the ISO, policies, or standards).
- Operate as information security monitors in their divisions or colleges.
- Attend and participate annually in data security steward training provided by the ISO.
- Be the primary point of contact for suspected or actual data breaches and report the information to the ISO.
- Promote information security events/training and generate a culture of information security awareness.
- Recommend employees with access to PII data to the ISO for additional levels of training.
- Provide recommendations for revisions to this policy as appropriate.

Employees, including department chairs, faculty, staff, and student workers - These individuals:

- Shall not disclose PII College data to unauthorized individuals.
- Shall not modify or delete College data unless authorized by the Data Owner to do so.
- Shall maintain College data in a secure manner.
- Shall complete the employee/student confidentiality training.
- Shall be required to sign a College confidentiality/FERPA agreement before access is granted to PII College data.
- Shall complete specific confidentiality training if they have job related responsibilities that require access to PII College data.

Network Security Administrator - This individual, within the IT Division will:

- Implement adequate security measures for computing systems containing College data within their jurisdiction.
- Implement appropriate security strategies for both the transmission and the storage of College data.
- Notify appropriate units of possible security infringements.
- Report any security breach to the ISO.
- Disseminate technical guidelines related to security to the appropriate IT Specialists.

Information Security Advisory Council – A group of individuals appointed by the President to review and evaluate College security issues such as:

- Current practices and the associated risks to the institution.
- Actions needed to address those risks through appropriate policy and associated guidelines.
- Identify new processes that are needed.
- Implement new security standards as needed.
- Disseminate general guidelines related to security to the appropriate IT specialists.
- Function as the incident response team
- Responsible for immediate response to any breach of security.
- Responsible for determining and disseminating remedies and preventative measures that are developed as a result of responding to and resolving security breaches.
- Report findings and recommendations regarding the incident to data stewards and College administration.

Information Security Office – This office, within the Business and Finance Division will:

- Assist the campus in identifying internal and external risks to the security and confidentiality of information.
- Provide guidance for handling College data in the custody of the College.
- Provide guidance for the security of the equipment or data storage devices where the information is processed and/or maintained.
- Promote and encourage good security procedures and practices.
- Develop and maintain Information security policy, plans, procedures, strategies, and best practices.
- Assist institutional or third-party auditors in the analysis of College information assets and IT resources to further ensure policy compliance.
- Provide standards and guidelines consistent with College policies.
- Develop and provide information security training.

Internal Auditor – Internal auditor will:

- Evaluate the effectiveness of the current safeguards for controlling security risks.
- Provide recommendations for revisions to this policy as appropriate.
- Develop and perform random audits of departments and individuals as deemed necessary.

APPENDIX B - STANDARDS AND GUIDELINES

ACCESS CONTROL

- Automatic logins may only be enabled on kiosks and digital signage. These are limited access accounts specifically designed for this purpose.
- PII, electronic or paper, must not be left in an accessible location to prevent unauthorized viewing and must be secured when unattended.
- All users of computing systems that contain College data must have their own user name and use a strong password. The sharing of user names and passwords is not allowed.
- The password of empowered accounts, such as system administrators, must be changed every 120 days or require multi-factor authentication.
- Passwords of standard College accounts, will automatically expire and require change after 360 days, if not changed during that period of time.
- College account access will automatically lock after 5 failed attempts. Accounts will automatically unlock after 5 minutes of inactive attempts.

- Passwords used for College access must not be the same as passwords used for personal accounts (banks, personal email, and credit cards).
- When resetting Password, users cannot reuse one of the previous 2 Passwords.
- Passwords must not be a user's Badger username, name or a word found in the dictionary.
- Passwords must not be placed in emails unless they have been encrypted.
- First-time passwords for new users must be set to a unique value for each user and changed after first use.
- Passwords must not be written down in a visible or accessible location.
- Periodic user access reviews should be conducted by the organization's supervisor and any unnecessary user access should be reported to IT Division and Human Resources and removed immediately.
- All workstations and lab computers must have a form of auto-lock feature enabled that requires a password to resume and set to activate at no more than an idle time of 20 minutes.
- Workstations visible to or accessible by anyone other than the authorized user must be manually locked when left unattended.

PHYSICAL SECURITY

- At a minimum, users shall comply with generally accepted College procedures to protect physical areas that contain College information.
- Individual organizations/departments within the College are responsible for physical security for personal computers and other local electronic information resources, including portable equipment, housed within their immediate work area or under their control.
- PII must only be used temporarily on portable equipment and then only for the duration of the necessary use and only if encrypted and physically secured.
- All College-owned computing equipment must be documented and managed in either a College-approved database or by property control.

DATA SECURITY

- All computing systems must install the College-approved management policy framework to manage antivirus and anti-spyware software as defined by the ISO in conjunction with the campus technology staff and leadership.
- PII data may only be stored on personal computers, servers or other computing equipment if the requirements outlined in USHE Policy R345, Information Technology Resource Security, are adhered to.

- All desktop systems and servers that connect to the network must be protected with a College-approved licensed anti-virus software product that is kept updated with the latest DAT files and anti-spyware software according to the vendor's recommendations.
- Headers of all incoming data, including electronic mail, must be scanned for viruses by the email server. Outgoing electronic mail must also be scanned for viruses.
- All servers must be approved and hardened with the IT Division before they will be allowed to transmit data through the Snow College firewall.
- Encryption technology will be utilized for local, portable, or central storage and transmission of PII.
- All transmission of PII via the Internet must be through a properly secured connection point to ensure the network is protected.
- All workstations and kiosks connected to the Internet will have a vendor supported version of the operating system installed with the option enabled to automatically download and install software updates or must utilize administrator managed patch management software.
- Software with the ability to serve information over the internet, must be disabled on all kiosks, workstations and lab computers.
- Peer-to-Peer (P2P) must be disabled on all kiosks, workstations, and lab computers.
- The file and printer sharing firewall exception must be disabled on all kiosks, workstations, and lab computers.

COMPUTING LABS

- All computing labs will utilize freezing or wiping software in such a way that minimizes the possibility of sensitive information from one user being accessible by any other user.