HILLSBORO AERO
ACADEMY

HILLSBORO AERO ACADEMY
INFORMATION SECURITY POLICY

Revised 2/14/21

I. PURPOSE

The purpose of the Information Security Policy is to:

- Provide policy to secure Sensitive Information of School employees, students, and others affiliated with the School, and to prevent the loss of information that is critical to the operation of the School.
- Provide reasonable and appropriate procedures to assure the confidentiality, integrity and availability of the School's Information Technology Resources.
- Prescribe mechanisms which help identify and prevent the compromise of information security and the misuse of School data, applications, networks and computer systems.
- Define mechanisms which protect the reputation of the School and allow the School to satisfy its legal and ethical responsibilities with regard to its networks' and computer systems' connectivity to networks outside the School.
- Provide written guidelines and procedures to manage and control information considered to be Sensitive Information whether in electronic, paper or other forms.
- Protect the integrity and validity of School data.
- Assure the Security and protection of Sensitive Information in the School's custody, whether in electronic, paper, or other forms.

School Information Technology Resources are a valuable School asset and must be managed accordingly to assure their integrity, security and availability for lawful educational purposes. This document describes policy for use by all persons and/or organizations that have access to School data.

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 as approved by the CEO/COO/CMO and Director of Compliance.

II. DEFINITIONS

A. 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, School databases, and faculty developed software for educational purposes) maintained by the IT Provider and located in areas managed by IT personnel.

B. Computing Equipment - All hardware used to process, store, or transmit School data.

C. Data - Information contained in either School computer systems or in physical copy that is utilized for the purposes of conducting School business or learning. The terms "data" and "information" are used interchangeably throughout this policy.

D. 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, School databases, and faculty developed software for educational purposes) maintained by any non- IT Division department.

E. 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.

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

G. 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.

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

I. Portable Equipment – Laptops and other removable storage devices such as Flash Drives.

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

K. 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.

L. Sensitive Information - 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 Hillsboro Aero Academy School interests, the conduct of School 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 School as requiring protective measures.

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

N. User – All persons and/or organizations that have access to School data.

O. Workstation - Computers assigned to one or more School employees for conduction School business.

III. SCOPE

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

This policy applies to all organizations within the School even though the data needed and used by those organizations are different. Additionally, all School 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.

Each department within the School must appropriately apply this policy to make certain they are meeting the requirements regarding Information Security.

Note: This policy applies to mobile devices as applicable.

V. ROLES AND RESPONSIBILITIES

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

VI. POLICY

A. 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.

B. Handling Sensitive Information

The unauthorized addition, modification, deletion, or disclosure of Sensitive Information included in School data files is expressly forbidden.

C. Centralized/Decentralized Computing Systems

All computing systems will be in compliance with this policy and School Security standards regardless of whether they are centralized or decentralized.

D. Sensitive Information Collection

Sensitive Information must only be collected for lawful and legitimate School purposes.

E. Public Information

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

F. Access Control

Access to School data and its resident computing system will be restricted to those users that have a legitimate business need and appropriate approvals for access to such information. Users must ensure that Sensitive Information 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.

G. Remote Access

Only authorized Users will be permitted to remotely connect to School computer systems, networks and data repositories to conduct School related business.

H. Physical Security

The physical security of computing resources will be accomplished utilizing current industry standards and appropriate technology and plans as defined by the IT provider. Responsibility for Centralized Computing systems security will reside with the IT Provider. See the Physical Security section of Appendix B for specific requirements.

I. Data Security

Users will ensure Sensitive Information is secure and the integrity of records is safeguarded in storage and transmission. Users who handle Sensitive Information 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.

J. Backup and Recovery

Administrators of Centralized computing systems will backup essential School data according to a documented disaster recovery plan consistent with industry standards and store such data at a secure commercial site.

K. Security Incident Response and Handling

All suspected or actual security breaches of School, college or departmental system(s) will be reported immediately to the organization's IT Provider to assess the level of threat and/or liability posed to the School or affected individuals and respond accordingly. The School will report and/or publicize unauthorized information disclosures as required by law or specific industry requirements.

L. Service Providers

Service providers utilized to design, implement, and service technologies must provide contractual assurance that they will protect the School's Sensitive Information it receives according to School or commercially reasonable standards.

Such contracts must be reviewed by School Legal Counsel for appropriate terminology regarding use and protection of Sensitive Information.

M. Training and Awareness

Each new School employee will be trained on the Acceptable Use Policy and School 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.

N. Computer Labs

Hillsboro Aero Academy provides computing lab resources for utilization in legitimate and lawful academic endeavors. Computing equipment in these areas will conform to all requirements of this policy with the addition of requirements stated in the Computing Lab Section of Appendix B.

O. Software

Only properly licensed software may be installed on School computer systems.

P. Penalties and Enforcement

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

Q. Policy Review and Revision

This policy and its associated appendices will be subject to periodic review and revision.

R. Policy Clarification

For clarification or further information on any items in this policy, the User is encouraged to contact their manager, the School IT Provider or the administrator liaison to the IR provider.

S. Additional Policies

Users should be aware that Oregon Higher Education Coordinating Commission may implement other policies that may affect Information Security on campus. The School adopts such policies and Users must comply with any such standards.

APPENDIX A – Roles and Responsibilities

Executive Directors/ Managers/Supervisors

These individuals shall be responsible for oversight of their employees' authorized use and access to School 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 School data is appropriate.
- Regularly review and document employee access to School data.
- Provide employees with resources and methods to properly secure equipment where School data is processed, stored, or handled.
- Provide employees with approved resources and methods for external data storage where School data is processed, stored, or handled.
- Notify appropriate units of possible Security infringements.
- Report any Security breach to the ISO.

Employees, including faculty, staff, and student workers

These individuals:

- Shall not disclose Sensitive Information to unauthorized individuals.
- Shall not modify or delete School data unless authorized to do so.
- Shall maintain School data in a secure manner.
- Shall be required to sign a School confidentiality/FERPA agreement before access is granted to Sensitive Information.

Information Security Office / IT Provider

This office will:

- Assist the School in identifying internal and external risks to the Security and confidentiality of information.
- Provide guidance for handling School data in the custody of the School.
- 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.
- Implement adequate Security measures for computing systems containing School data within their jurisdiction.
- Implement appropriate Security strategies for both the transmission and the storage of School data.
- Notify appropriate units of possible Security infringements.
- Develop and maintain Security policy, plans, procedures, strategies, and best practices.
- Provide standards and guidelines consistent with School policies.
- Develop and provide Information Security training.

Internal Audit

Internal Audit 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.

- Sensitive information, 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 School 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.
- Passwords used for School access must not be the same as passwords used for personal accounts (banks, personal email, and credit cards).
- Passwords must not be a User's system 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 20 minutes idle time.
- 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 School procedures to protect physical areas that contain School information.
- Individual Organizations/Departments within the School 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.
- Sensitive Information 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 School owned computing equipment must be documented and managed in either a School approved database or by Property Control.

Data Security

- All computing systems must install the School approved management policy framework to manage antivirus and anti-spyware software as defined by the IT Provider.
- Sensitive Information may only be stored on personal computers, servers or other computing equipment if the requirements outlined in BOR R345, Information Technology Resource Security, are adhered to.
- All desktop systems and servers that connect to the network must be protected with a School 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 registered with the IT Provider before they will be allowed to transmit data through the Hillsboro Aero Academy School firewall.
- Encryption technology will be utilized for local, portable or central storage and transmission of Sensitive Information.
- All transmission of Sensitive Information 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.
- Internet Information Services (IIS) 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.