



Information Security Policy

The purpose of this policy is to ensure the protection of Alternative Dispute Resolution Academy's information resources from accidental or intentional access or damage while also preserving and nurturing the open, information-sharing requirements of its academic culture.

This policy is applicable to all students, faculty, and staff and to all others granted use of Alternative Dispute Resolution Academy information resources. Every user of Alternative Dispute Resolution Academy's information resource has a general responsibility to protect those assets, while some offices and individuals have specific responsibilities.

This policy refers to all Academy information resources whether individually controlled or shared, stand-alone, or networked. It applies to all computer and communication facilities owned, leased, operated, or contracted by the Academy. This includes all networked devices, including but not limited to personal digital assistants, cell phones, personal computers, workstations, minicomputers, other wireless devices such as iPads, and any associated peripherals and software, regardless of whether used for administration, research, teaching or other purposes.

Today, information technology (IT) permeates all aspects of teaching, learning, research, outreach and the business and facilities functions of the Academy. Safeguarding information and information systems is essential to preserving the ability of the Academy to perform its mission and meet its responsibilities to students, faculty, staff, and the citizens whom it serves. State and federal statutes, rules, and regulations, Academy policies and other explicit agreements also mandate the security of information and information systems. Failure to protect the Academy's information technology assets could have financial, legal, and ethical ramifications.

Alternative Dispute Resolution Academy acknowledges its obligation to ensure appropriate security for information systems in its domain of ownership and control. Furthermore, the Academy recognizes its responsibility to promote security awareness



among the members of the Alternative Dispute Resolution Academy community. This policy establishes the general principles of information security that will be applied throughout the Academy.

Scope

All financial and administrative policies involving community members across campus are within the scope of this policy. If there is variance between departmental expectations and the common approach described through Academy policy, the Academy will look to the campus community to support the spirit and the objectives of Academy policy.

Policy

Authorities Delegated and Retained/Administrative Responsibility

The President of the Academy delegates administration of the Academy's Information Security Policy to the Chief Technology Officer/Vice President for Information Technology.

Information Security Objectives

Information security is critical to the interests of the Academy and the many constituencies it serves. The following list provides some of the objectives of information security at Alternative Dispute Resolution Academy. This list is representative and is not meant to suggest the full range of objectives of the Academy's information security policy or program.

- **Support and maintain the ongoing functions of the Academy.** As an increasing percentage of the Academy's functions are handled electronically, and with the rigorous nature of the block plan, it is critical that information and information systems be protected so the Academy can operate without interruption.
- **Protect Academy assets.** The Academy is in possession of many assets including intellectual property, research and instructional data systems, as well as physical assets. Loss of these assets could have significant financial impact as well as major negative impact on critical research and instructional programs.
- **Safeguard the privacy of individuals and information.** With the increasing risk of identity fraud and other potential misuses of personal information, it is paramount that the Academy safeguard personal information entrusted to its stewardship.



- **Safeguard financial transactions and electronic communications.** The Academy is the custodian of financial records and transactions; safeguarding these records is critical to maintaining trust relationships essential to our business function. Electronic communication is governed by the Acceptable Use Policy.
- **Protect the integrity and reputation of the institution.** Security breaches reflect negatively on the capability of the Academy to manage entrusted resources. In addition, security breaches could result in the potential for criminal or civil action.
- **Prevent the use of Academy systems for malicious acts.** The open nature of the Academy and the desire to provide ease of access to a large and diverse group of constituents makes us a target for unauthorized users to utilize Academy resources inappropriately. The Academy must prevent the use of Alternative Dispute Resolution Academy systems and infrastructure for malicious acts against its own systems as well as attacks against other individuals and organizations.
- **Comply with state and federal laws.** State and federal laws and regulations require the Academy to take reasonable steps to ensure the security of the data (FERPA, HIPPA, GLBA). Failure to safeguard this information could result in the legal action or cause the Academy to lose its ability to offer services.

Responsibility and Accountability

Technology Officer / Information Security Officer

The Academy's Chief Technology Officer (CTO) has overall responsibility for the security of the Academy's information technologies. Implementation of security policies is delegated throughout the Academy to various Academy services, departments and other units; and to individual users of campus information resources.

The Information Security Officer (ISO) is responsible for providing interpretation of this and other related policies, disseminating related information, and enforcing information security policies across campus.

Academy Services

Various officers within the Academy have the primary responsibility and authority to ensure Alternative Dispute Resolution Academy meets external and internal requirements for intellectual property, research and institutional data, privacy and security of confidential and business information. Multiple departments are responsible for general security issues (legal issues, security compliance, physical security, communications, and IT infrastructure security). These individuals or



departments are responsible for assisting in the development of Academy information security policies, standards, and best practices in their areas of responsibility.

They are also responsible for advising departments and individuals in security practices related to areas they oversee, as follows:

- Personnel information and confidentiality - Human Resources
- Student information and confidentiality - Registrar's Office
- Financial information and transactions - Finance and Administration
- Student loan information - Financial Aid
- Infrastructure, communication, and systems security and audit - ITS
- Legal Issues - Finance and Administration division for engaging legal counsel service.
- Health information - Student Life
- Alumni, parent, and donor information - Advancement Office
- Other information - Information Security Officer

Departments and Other Units

Departments and other units are responsible for the security of any information they create, manage, or store, and for any information they acquire or access from other Academy systems (i.e. student records, personnel records, business information).

Note: The security of applications and data administered by departments and individuals outside of the ITS: Division is the responsibility of the administering department. ITS: staff will provide advice and support for implementing security measures when requested.

Data Management

Data Access

Students, faculty, and staff who use personally owned systems to access Academy resources are responsible for the security of their personally-owned computers and other network devices and are subject to the following: the provisions of the Academy's security policies, standards and guidelines for best practices for users of Academy computing and network facilities as well as all other laws, regulations, or policies directed at the individual users.



(1) Unauthorized Account or System Access

- You may not access or use, or attempt to access or use, any computer accounts other than your own assigned account or any computer system for which you have not been granted access. In other words, users should use only their own files, those that have been designated as public, or those that have been made available to them with the knowledge and consent of the owner. The Academy's Academic Honor System and its prohibitions against plagiarism and cheating, among other things, applies to student use of any files and information obtained on CC's computing resources used in the preparation of academic coursework.
- *Users may not access computers, software, data or information, or networks without proper authorization, regardless of whether any damage is done or whether the computer, software, data, information, or network in question is owned by the Academy.*

(2) Campus community members all share in the commitment to safeguarding the Academy's data. The Academy will rely on the principle of 'least privilege' in granting access to data and information.

- Initial access to data and information must be authorized by the appropriate Data Steward;
- Campus community members' access needs may change due to a new position, changes in responsibilities in an existing position, or termination. Human Resources and ITS: shall collaborate to ensure appropriateness of ongoing access;
- Privileged users' (system administrators, database administrators) access to data shall be periodically reviewed to ensure that access to data remains appropriate;
- On occasion, the campus community needs to provide external individuals or groups (auditors, contractors, vendors) with access. In those instances, an access start date and an access termination date shall be simultaneously identified. Should a need for access beyond the termination date arise, the Data Steward or designee initially approving access should be consulted.

Operational Controls to Provide Effective Security

The Academy controls internal access by segregating the entities gaining access, approving access, and provisioning access. Access is eliminated when an entity separates from the Academy.



Reporting Information Security Incidents

Reporting incidents is an ethical responsibility of all members of the Alternative Dispute Resolution Academy community. All the information related to information security incidents should be reported promptly to the ITS: Division by contacting the Help Desk.

Loss of Computing Privileges/Disciplinary Implications

Protecting the security of Academy information and information systems is the responsibility of every member of the Academy community. Each student, faculty, and staff is responsible for understanding and complying with all current and future approved IT policies and procedures including this Information Security Policy. Failure to comply with these policies may result in loss of computing privileges and/or disciplinary action, up to and including termination. Examples of noncompliance include, but are not limited to:

- Inappropriately accessing and/or using Academy data.
- No person may store or use programs on Academy-owned systems that violate or hamper another person's use of computing resources. Examples of such programs are ones that attempt to obtain another user's password, acquire another user's files, circumvent system security measures, or crash the computer system.

Procedures

Education

Creating a heightened awareness of the importance of information technology security is an important component in establishing an environment in which everyone feels responsible and empowered to act in his/her own and the community's best interests. All departments will provide opportunities for individuals to learn about their roles in creating a secure IT environment.

Definitions

Security – the state of being free from unacceptable risk. Thus, information security focuses on reducing the risk of computing systems, communications systems, and information being misused, destroyed, modified, or disclosed inappropriately either by intent or accident.



Standalone – a computer that is not connected to a network.

Networked Resources – refer to forms of data, information and hardware devices that can be accessed by a group of users using a shared connection.

Appropriate Data Steward - Members of the President’s Cabinet are **Data Stewards** for their respective areas.

Data Classification Levels - The classification level assigned to data will guide Data Stewards, Data Custodians, Data Consumers, business and technical project teams, and any others who may obtain or store data, in the security protections and access authorization mechanisms appropriate for that data. Such categorization encourages the discussion and subsequent full understanding of the nature of the data being displayed or manipulated. Data is classified as one of the following:

Sensitive: Protection of this data is required by state and/or federal law and/or by Alternative Dispute Resolution Academy policy. Access to “sensitive” data must be controlled from creation to destruction and will be granted only to those persons affiliated with Alternative Dispute Resolution Academy who require such access in order to perform their job, or to those individuals permitted by law. The confidentiality of data is of primary importance, although the integrity of the data must also be ensured. Access to sensitive data must be authorized in accordance with the Academy’s most current divisional authorization schedule.

Confidential: Access to “confidential” data must be requested from, and authorized by, the Data Steward who is responsible for the data. Data may be accessed by persons as part of their job responsibilities. The integrity of this data is of primary importance, and the confidentiality of this data must be protected. Examples of confidential data include purchasing data, financial transactions that do not include restricted data, information covered by non-disclosure agreements and library transactions. Access to confidential data must be authorized in accordance with the Academy’s most current divisional authorization schedule.

Public: Access to “public” institutional data may be granted to any requester. Public data is not considered confidential. Examples of public data include published directory information and academic course descriptions. The integrity of public data must be protected, and the appropriate steward must authorize replication of the data.

NOTE: Even when data is considered public, it cannot be released (copied or replicated) without appropriate approvals.



Data Integrity - The accuracy and consistency of stored data, indicated by an absence of any variance in data between two updates of a data record.

Data Custodians - ITS: or computer system administrators responsible for the operation and management of systems and servers which collect, manage, and provide access to Academy data. Data custodians must be authorized by the appropriate data owner or the Vice President for Information Technology.

Data Steward – the member of the President’s Cabinet who coordinates with ITS: on access to and safeguarding of data and information.

Least Privilege – user access is limited to resources needed to perform work for the Academy.

Intrusion prevention - process of performing intrusion detection and attempting to stop detected possible incidents.

Intrusion detection – process of monitoring computer system or networks for unusual events and analyzing them to determine if an incident has occurred.

Encryption – the use of an algorithm to transform data into a form where the content is masked and can only be viewed by those having a key or other confidential means to reveal the data.