DaVinci Academy of Science and The Arts

Policy Number: 705
Policy Section: 700 – Technology

POLICY TITLE: Electronic Information Security Policy

Revision History

Effective Date	Action Date	Revised
8 October 2008	New Policy	New Policy

Electronic Information Security Policy
Effective Date: 17 September 2008
Revision Date:

1. OVERVIEW

1.1 Protection of DaVinci Academy information assets and the technology resources that support the school is critical to the functioning of the DaVinci Academy. DaVinci Academy information assets are at risk from potential threats such as employee error, malicious or criminal action, system failure, and natural disasters. Such events could result in damage to or loss of information resources, corruption or loss of data integrity, interruption of the activities of DaVinci Academy, or compromise to confidentiality or privacy of members of the school community.

1.2 These Electronic Information Security guidelines seek to reduce risks to electronic information resources through implementation of controls designed to detect and prevent errors or irregularities that may occur. DaVinci Academy recognizes that absolute security of electronic information resources against all threats is an unrealistic expectation that would require the commitment of a prohibitively high level of resources.

1.3 The School's goals for risk reduction are based, therefore, on the principle that the level and type of security should reflect an assessment of:

1. the criticality of an Electronic Information Resource to the operation of DaVinci Academy;
2. the sensitivity of the data residing in or accessible through the Electronic Information Resource;
3. the cost of preventive measures and controls designed to detect errors or irregularities; and

1.4 Achieving a successful information security program requires management planning for preparedness, detection, response and recovery with respect to protection of the information enterprise. Risk assessment and determination of appropriate security measures must be a part of all systems design and operations.

1.5 These guidelines identify the set of measures that should comprise schools security programs. Security programs should include identification of the Electronic Information Resource IT Manager and possible support staff such as students or dedicated personal that is responsible for school compliance with its security program. Security programs shall undergo periodic evaluation of administrative, technical, and physical safeguards to ensure that they adequately address operational or environmental changes.

1.6 These Guidelines include sections that address the following:

1. Definitions - a list of terms used in these Guidelines and defined in Appendix A.

2. Scope - the scope of these Guidelines.
3. Risk Assessment, Sensitivity and Criticality - a taxonomy of the *sensitivity* of electronic information resources and the *criticality* of information resources, to be used for assessing risk, incident response planning, and notification in instances of security breaches.
4. Disaster Recovery and Emergency Procedures - a description of requirements for Disaster Recovery Plans and emergency procedures.
5. Logical Security - security measures for controlling access to electronic information resources through logical means (e.g., via software or network controls), procedural controls related to software development and change control, security of data (including encryption), communications security, and reduction of risk from intrusive computer software.
6. Physical Security - security measures for controlling access to electronic information resources through physical means, including disaster controls, physical access controls, device and media controls, and procedural controls over financial instruments (e.g., check stock) and maintenance records.
7. Managerial Security Measures - security measures with respect to employment and other organizational matters, actions to be taken with respect to suspected violations of these Guidelines, and workforce security and awareness training.
8. Responsibilities - responsibilities for maintenance and implementation of these Guidelines.
9. Summary of Campus Responsibilities - a summary of the campus responsibilities for implementing these Guidelines.

2. DEFINITIONS

2.1 The following terms used in these Guidelines are defined in Appendix A. Knowledge of these definitions is important to an understanding of these Guidelines.

Authorized User
Business Continuity Plan
Computer Virus
Disaster
Disaster Recovery Plan
Electronic Information Resource
Electronic Information Resource IT Manager
Electronic Information Resource Proprietor (IT Manager)
Electronic Information Resource Security (IT Manager)
Intrusive Computer Software
Security
Server
User

3. SCOPE

3.1 These Guidelines apply to all of the School of DaVinci Academy, including Custodial to the BDASA Board and the Director of Academics. Implementation of these

Guidelines, including development of more specific standards or guidelines as needed, is the local responsibility of the DASA IT Manager.

3.2 The IT Manager in its system wide role across DaVinci Academy has overall responsibility for establishing policy, including these Guidelines on Electronic Information Security.

3.3 These Guidelines apply to the security of Electronic Information Resources, as defined in Appendix A, Definitions. Electronic Information Resources include application systems, operating systems, tools, communications systems, data – in raw, summary, and interpreted form – and associated computer mainframe, server, desktop, communications and other hardware used to conduct activities in support of the DaVinci Academy mission and vision.

3.4 The related DaVinci Academy policies and procedures that cover issues related to Records Retention, Vital Records, Data Privacy, allowable use of Electronic Information Resources, and Investigation of Misuse of DaVinci Academy Resources are written and published by the DASA IT Manager under the discretion of the DASA Executive board and the Director of Academic services.

4. RISK ASSESSMENT, SENSITIVITY AND CRITICALITY

4.1 The schools IT Manager shall ensure that risk assessments are conducted to identify the Electronic Information Resources that require protection, and to understand and document risks from security failures that may cause loss of confidentiality, integrity, or availability; risk assessments should take into account the potential adverse impact on the DaVinci Academy's reputation, operations, and assets. Risk assessments should be conducted by teams composed of appropriate administrators, managers, faculty, and information technology and other personnel associated with the activities subject to assessment.

4.2 When determining the level of security required for an Electronic Information Resource, there are two basic risk characteristics to be assessed:

1. The level of *sensitivity* of the Electronic Information Resource; and
2. The level of *criticality* or overall importance of the Electronic Information Resource to the continuing operation of the DaVinci Academy School.

4.3 The level of access controls required for an Electronic Information Resource depends on the *sensitivity* of the Electronic Information Resource, as defined below. The requirement to include a particular Electronic Information Resource in Disaster Recovery Plans as part of overall business continuity planning depends on the *criticality* of the application to the DaVinci Academy.

4.4 Data Proprietors must ensure that the release of sensitive data to authorized users is accompanied with instructions regarding appropriate use and protection.

5. ELECTRONIC INFORMATION RESOURCE SENSITIVITY

5.1 The sensitivity of an Electronic Information Resource, and therefore the level of security required, depends upon the sensitivity of the data retained by or accessible through the Electronic Information Resource.

Note: A security designation under these Guidelines shall have no effect on the treatment, consideration or disclosure of any document or information under state or federal law, including the Utah Public Records Act, the Utah Information Practices Act, the Family Educational Rights and Privacy Act of 1974 (FERPA), and the Health Insurance Portability and Accountability Act of 1996 (HIPAA).

1. Data falls into one of two levels of sensitivity: Restricted or Unrestricted. The Electronic Information Resource Proprietor is responsible for determining the level of sensitivity of data based on:
2. The level of security required for protecting the data from unauthorized read-only access; and
3. The level of security required for protecting the data from unauthorized creation, deletion, or modification, collectively termed "modification" for purposes of these Guidelines.

6 RESTRICTED DATA

6.1 Restricted data is data that is considered sensitive to some degree. It is divided into two subcategories: ***Personal* and *Limited.***

6.2 **Personal** data refers to the combination of any information that identifies and describes an individual, including but not limited to, his or her name, social security number, protected health information (PHI), School records such as transcripts, Special education records and financial account information. Access to such data is governed by state and federal laws, both in terms of protection of the data, and requirements for disclosing the data to the individual to whom it pertains. Protection for such data may also be subject to additional operating regulations in accordance with vendor or partner agreements, such as the Payment Card Industry Data Security Standards.

6.3 **Limited** refers to:

1. Electronic information whose unauthorized access, modification or loss could seriously or adversely affect the school (e.g., cause financial loss or loss of confidence or public standing in the community), adversely affect a partner (e.g., a business or agency working with the School), or adversely affect the public. Examples of such data may include selected research data where the corresponding research is incomplete, or responses to a Request for Proposal before a decision has been reached.

2. Electronic information that the Electronic Information Resource Proprietor chooses to protect from general access or modification, although such access is not prohibited by law or DaVinci Academy policy. An example might include data containing budget projections for a campus department or DASA Board information of any kind.

7. UNRESTRICTED DATA

7.1 Unrestricted data is data for which access or modification is not restricted by law or DaVinci Academy policy and is permitted by the Electronic Information Resource.

7.2 Proprietor. Examples of data that are Unrestricted from the standpoint of access include data contained in annual school financial reports, class catalogs, and the schools general information handbooks.

7.3 Unrestricted data that pertains to individuals equates to "non personal" information.

7.4 The same data may be classified differently for different purposes. Thus, a staff member's office address may be Unrestricted for read-only access but Restricted for modification. A *Restricted Electronic Information Resource*, as used in the remainder of these Guidelines, is an Electronic Information Resource for which the data retained within the resource or accessible through the resource is considered Restricted for either read-only access or for modification access.

7.5 DaVinci Academy must implement procedures to provide security for Restricted Electronic Information Resources (see Section VI, Logical Security and Section VII, Physical Security).

8. ELECTRONIC INFORMATION RESOURCE CRITICALITY

8.1 Electronic Information Resource criticality is a measure of the importance of an Electronic Information Resource to the continuing operation of a campus. The criticality of an Electronic Information Resource determines whether or not it must be included in a school Disaster Recovery Plan (see Section V, Disaster Recovery and Emergency Procedures). Electronic Information Resources are classified into three levels of criticality as follows:

1. **Essential:** An Electronic Information Resource should be designated as *Essential* if its failure to function correctly and on schedule could result in a major failure by a campus to perform mission-critical business functions, a significant loss of funds to the school, or a significant liability or other legal exposure to the school.
2. **Required:** An Electronic Information Resource should be designated as *Required* if it performs an important function for the school, but the operation of the school could continue for some designated period of time without the function

provided by the Information Resource and there is time for recovery should the Information Resource not perform correctly or on schedule.

3. **Deferrable:** An Electronic Information Resource should be designated *Deferrable* if the school could continue operation for an extended period of time without the Information Resource performing correctly or on schedule.

8.2 The Payroll and Personnel System (as put into place by the DASA Board, the DASA Business Manager or the DASA Academic Director), the schools data network and the telephone and public safety communication systems should be considered Essential systems at the DaVinci Academy School. An example of an Electronic Information Resource that is likely to be considered Essential by the school is the states SIS system or the DaVinci Academy's Email system or the DaVinci Academy's school Quick books system.

8.3 The same Electronic Information Resources may be designated Essential, Required, or Deferrable depending on the period of inoperability. For example, General Ledger monthly financial reporting may be deemed Deferrable, but financial reporting at fiscal year-end would be considered Essential.

8.4 DaVinci Academy must include all Essential Electronic Information Resources in a schools Disaster Recovery Plan (see Section V, Disaster Recovery and Emergency Procedures).

8.5 The designation Essential, Required, or Deferrable may be applied to various types of Electronic Information Resource. For example, these Guidelines also refer to Essential applications or Required servers.

9. SUMMARY CHART

The security requirements of Data Sensitivity and Electronic Information Resource Criticality are summarized below:

	Electronic Information Resource Criticality			
	Essential	Required		Deferrable
Data Sensitivity	Restricted	Requires access security; must be in Disaster Recovery plan	Requires access security; may be in Disaster Recovery plan	Requires access security; need not be in Disaster Recovery plan
	Unrestricted	Minimal security required; must be in Disaster Recovery plan	Minimal security required; may be in Disaster Recovery plan	Minimal security required; need not be in Disaster Recovery plan