10
2009

**Index**

Protecting Records P.1
FERPA P.2
Record Disclosure P.3
Recommendations P.4
Securing Access P.5
PKI Management P.6
Accountability P.7

digicert®
Your Success is Built on Trust™

# Protecting the Security of Education Records

**White Paper**

This white paper presents a brief survey of legal and information security issues that may arise when handling records of students, parents, faculty and staff at learning institutions.

**Who, besides the IT Department, should read this White Paper?**

Registrars and departments of human resources at educational institutions play an important role in securing personal information.

Registrars are the initial and primary custodians of student data. Registrars also typically control the granting and denial of access to student personal data, and should be familiar with federal and state regulations related to the privacy and protection of student records.

Similarly, a department of human resources will collect and control the use of personal information of faculty and staff. These two groups should be aware of the legal and information security risks of data custodianship created by collecting and managing this important information.

## Introduction

Academic and administrative computing systems used to be more isolated—either intentionally for security reasons or as a result of limited interconnectivity with other computers—but today it seems that nearly any information that an administrator, teacher, student or parent might need can be obtained through a network connection. Course materials are presented and students submit their assignments via the Internet (see “FERPA Regulations” in sidebar), school lunch accounts and student grades can be accessed by parents online, and administrative paperwork and other information is shared among a variety of systems and people in K-12 and higher education. The Internet is a great way to communicate, but it introduces security threats that did not threaten walled-off systems of the last century.

Now that registration, application materials and grades are submitted and recorded over open networks, better security measures are needed. However, the need for better information security can conflict with the need for academic freedom and access to information. It is also challenging to keep pace with a continually changing computing environment.

Faster processors and better software continue to be introduced into the computing environment, but methods used by hackers and the authors of malicious software also advance.

> ***Computer systems at colleges and universities have become favored targets because they hold many of the same records as banks but are much easier to access.***
>
> *73 Federal Register 74,806, 74,843 (December 9, 2008)*

Thus, constant vigilance and security oversight are needed now more than ever.

As school administrators are faced with the need to meet legal and business requirements related to information security, regulatory frameworks also drive the adoption of security policies. These regulatory frameworks can be numerous and daunting at times. Take for instance FERPA, HIPAA, GLBA, PCI- DSS, the breach notification laws of 45 different states, and various EU Data Protection laws. This white paper focuses on FERPA and state data breach notification laws (leaving for other white papers a discussion of HIPAA, GLBA, PCI-DSS, breach notification, and laws in the EU). It then discusses industry best practices, which also channel information security decisions for schools.





DigiCert, Inc.
355 South 520 West
Canopy Building II
Lindon, UT 84042
+1-800-896-7973 ph
www.digicert.com

# The Family Educational Rights and Privacy Act (FERPA)

**"Education Records"**

FERPA grants parents (e.g., parents of students K-12) and eligible students (at least 18 years old or attending school beyond the high school level) the right to inspect and review "education records" and protects their right to privacy by limiting the disclosure of such education records to certain situations. The term "education records" is defined in 34 C.F.R. § 99.3 as "those records that are: (1) Directly related to a student; and (2) Maintained by an educational agency or institution or by a party acting for the agency or institution." This includes financial information submitted to the school by the student's parents, but excludes alumni records collected and maintained by alumni associations because they are not directly related to the individual as a student.

**"Directory Information" and Social Security Numbers**

Nevertheless, FERPA permits the disclosure of "directory information" (unless the parent or eligible student has opted out of such information sharing). Directory information includes name, address, phone number, email, and a student ID number if it cannot be used to gain access to education records except when used with one or more other factors to authenticate the user's identity.

According to 34 C.F.R. § 99.3, "directory information" does not include a student's— (1) Social security number; or (2) Student identification (ID) number, except as provided in paragraph (c) of this section.

(c) Directory information includes a student ID number, user ID, or other unique personal identifier used by the student for purposes of accessing or communicating in electronic systems, but only if the identifier cannot be used to gain access to education records except when used in conjunction with one or more factors that authenticate the user's identity, such as a personal identification number (PIN), password, or other factor known or possessed only by the authorized user. 34 C.F.R. § 99.3.

FERPA prohibits a school from using a student's social security number when disclosing or verifying directory information. In other words, when releasing or confirming directory information about a student, the school may not use non-directory information to identify the student or locate the directory record, even when it is supplied by the requester, unless a parent or eligible student has provided written consent. This is because confirmation of information in education records is considered a disclosure under FERPA. See 20 U.S.C. 1232g(b). Otherwise, the school may use the student's name, address, date of birth, school, class, year of graduation, and other directory information to identify the student or locate the student's records.

**FERPA Requires that Schools Maintain "Direct Control" over the Disclosure of Education Records to Outside Parties**

FERPA generally prohibits disclosure of education records to "outside parties" without prior consent. However, recently the U.S. Department of Education has clarified that prior consent is not required to disclose education record information to a contractor, consultant, volunteer, or other party provided that the other party meets the requirements of § 99.31(a)(1)(B)(2) (the outside party must be under the direct control of the agency or institution with respect to the use and maintenance of information from education records). "Once a school has determined that an outside party is a ''school official'' with a ''legitimate educational interest'' in viewing certain education records, that party may have access to the education records, without consent, in order to perform the required institutional services and functions for the school. These outside parties may include parents and other volunteers who assist schools in various capacities, such as serving on official committees, serving as teachers' aides, and working in administrative offices, where they need access to students' education records to perform their duties." 73 Fed. Reg. at 74,814.

**About FERPA**

The Family Educational Rights Privacy Act (FERPA) was enacted in 1974. It prohibits educational institutions from disclosing certain sensitive "personally identifiable education information" and gives parents the right to receive access to their children's education records. These rights are subsequently transferred to students when they turn 18 years of age. FERPA also requires schools to track disclosures of education records to third parties.

**FERPA Regulations**

FERPA Regulations can be found in Section 99 of Title 34 of the Code of Federal Regulations. Importantly, they now define "attendance" as "videoconference, satellite, *Internet, or other electronic information and telecommunications technologies* for students who are not physically present in the classroom."

34 C.F.R. § 99.3.

**What's New With FERPA?**

On December 9, 2008, the U.S. Department of Education revised its FERPA regulations in the areas of:

- Authentication of users
- Access control over data
- Controls over third parties
- Measures to safeguard data





DigiCert, Inc.
355 South 520 West
Canopy Building II
Lindon, UT 84042
+1-800-896-7973 ph
www.digicert.com

# Disclosure of Education Records to Third Parties

**FERPA-Compliant Outsourcing Contracts**

"Under the regulatory framework for redisclosing education records in § 99.33(b), educational agencies and institutions retain primary responsibility for disclosing and authorizing redisclosure of their education records without consent." 73 Fed. Reg. at 74,821.

"Schools outsourcing information technology services, such as web-based and e-mail services, should make clear in their service agreements or contracts that the outside party may not use or allow access to personally identifiable information from education records, except in accordance with the requirements established by the educational agency or institution that discloses the information." 73 Fed. Reg. at 74,816.

Under 34 C.F.R. § 99.32(b), the school must record the names of the additional parties to which the receiving party may redisclose the information on behalf of the school and their legitimate interests under § 99.31. Thus, any outsourcing arrangement should consist of a service contract that explicitly delineates the role of the school, the permitted use of the information, and the importance of information security in preventing the unauthorized disclosure of student records.

**Disclosure Recordkeeping and Breach Notification**

The threat of a data breach presents a reputation risk to the school regardless of whether data is ultimately used--it can harm the school's reputation and also cause breach notification and legal defense costs. Fortunately, courts have rejected tort claims based on the disclosure of personal data where there has been no actual use of the data for identity theft (because plaintiffs have lacked financial injury or other damages).

Section 99.32(a)(1) of 34 C.F.R. only requires recordkeeping of information disclosures: "An educational agency or institution must maintain a record of each request for access to and each disclosure of personally identifiable information from the education records of each student, ...."

However, schools must still comply with other federal and state laws requiring notification to individuals if certain types of their personally identifiable information are disclosed.

A plethora of state laws require notification in the event of a data breach. As of the date of this White Paper, at least 45 states have adopted breach notice laws, along with the District of Columbia, Puerto Rico, and the U.S. Virgin Islands. http://www.ncsl.org/programs/lis/cip/priv/breachlaws.htm. These laws typically cover disclosures of names, social security numbers, driver's license and credit card numbers, which may give another person access to financial information or a greater ability to commit identity theft. Because colleges and universities maintain data on out-of-state residents for admissions, financial aid and alumni purposes, it is more likely than not that multiple state laws will apply in the event of a data breach.

Also, health records are now covered by the data breach notification requirements of Title XIII of the American Recovery and Reinvestment Act of 2009, known as the HITECH Act. Section 13402 of the HITECH Act requires that notifications be made without unreasonable delay but in no case later than 60 calendar days after discovery of the disclosure of unsecured protected health information.

**FERPA (Continued)**

**Disclosure** means "to permit access to or the release, transfer, or other communication of personally identifiable information contained in education records by any means, including oral, written, or electronic means, to any party except the party identified as the party that provided or created the record." 34 C.F.R. § 99.3.

**Direct control** is not defined. Must the school monitor the operations of the outside party? Should it verify that outside parties have the necessary resources to safeguard education records provided to them? Must the outside party agree by contract to implement appropriate safeguards?

In response to these questions, the Department of Education has said that the institution should not disclose education records "unless it can control that party's maintenance, use, and redisclosure of education records." "We believe that the use of the 'direct control' standard strikes an appropriate balance in identifying the necessary and proper relationship between the school and its outside parties that are serving as 'school officials.' " 73 Fed. Reg. 74,806, 74,816 (Dec. 9, 2008).





DigiCert, Inc.
355 South 520 West
Canopy Building II
Lindon, UT 84042
+1-800-896-7973 ph
www.digicert.com

# U.S. Department of Education Recommendations for Data Breach Situations

While FERPA does not have breach notification requirements, the risks of data breaches have not been ignored by the U.S. Department of Education:

If an educational agency or institution has experienced a theft of files or computer equipment, hacking or other intrusion, software or hardware malfunction, inadvertent release of data to Internet sites, or other unauthorized release or disclosure of education records, the Department suggests consideration of the following steps:

• Report the incident to law enforcement authorities.

• Determine exactly what information was compromised, i.e., names, addresses, SSNs, ID numbers, credit card numbers, grades, and the like.

• Take steps immediately to retrieve data and prevent any further disclosures.

• Identify all affected records and students.

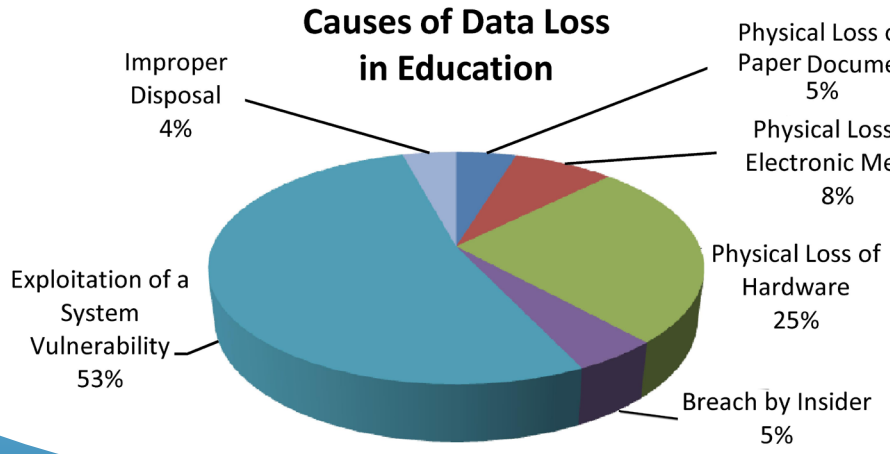
• Determine how the incident occurred, including which school officials had control of and responsibility for the information that was compromised.

• Determine whether institutional policies and procedures were breached, including organizational requirements governing access (user names, passwords, PINS, etc.); storage; transmission; and destruction of information from education records.
• Determine whether the incident occurred because of a lack of monitoring and oversight.

• Conduct a risk assessment and identify appropriate physical, technological, and administrative measures to prevent similar incidents in the future.

• Notify students that the Department's Office of Inspector General maintains a Web site describing steps students may take if they suspect they are a victim of identity theft at http://www.ed.gov/about/offices/list/oig/misused/idtheft.html; and http://www.ed.gov/about/offices/list/oig/misused/victim.html.

FERPA does not require an educational agency or institution to notify students that information from their education records was stolen or otherwise subject to an unauthorized release, although it does require the agency or institution to maintain a record of each disclosure. 34 CFR 99.32(a)(1). (However, student notification may be required in these circumstances for postsecondary institutions under the Federal Trade Commission's Standards for Insuring the Security, Confidentiality, Integrity and Protection of Customer Records and Information ("Safeguards Rule") in 16 CFR part 314.) In any case, direct student notification may be advisable if the compromised data includes student SSNs and other identifying information that could lead to identity theft. 73 Fed. Reg. at 74,844.




**Pie Chart Data:** Curtin & Ayers, "Using Science to Combat Data Loss: Breaches by Type and Industry," Journal of Law & Policy for the Information Society, p. 32 from web.interhack.com

## DigiCert's Additional Recommendations

• Preserve and collect evidence of the breach for forensic processing by computer crime lab;

• Determine which state laws apply and whether the HITECH Act applies and comply with breach notice requirements in those laws;

• Determine the level of risk of identity theft to data subjects, including the ease/difficulty in accessing the data in light of manner in which it was stored, how the loss occurred, the ability to mitigate potential identity theft, and whether any identity theft is actually occurring;

• Be prepared with an incident response plan, including employee training and identification of outside contractors who may be able to help you respond to breach notice obligations;

• Designate a contact person who will have all of the information and authority necessary to coordinate the public release of information about the breach;

• View the breach and notice from the perspective of those who have had their data compromised—this will help you provide a notice that adequately addresses concerns and answers questions that might otherwise arise; and

• Be honest and straight-forward—this will help build trust and put the event behind you.





DigiCert, Inc.
355 South 520 West
Canopy Building II
Lindon, UT 84042
+1-800-896-7973 ph
www.digicert.com

# Securing Access to Education Records

**Implementing Physical, Technological and Administrative Security Controls**

Section 99.31(a)(1)(ii) of Title 34 C.F.R. requires that schools "use reasonable methods to ensure that school officials obtain access to only those education records in which they have legitimate educational interests." The U.S. Department of Education has explained "reasonable methods" as follows:

> *We believe that the standard of 'reasonable methods' is sufficiently flexible to permit each educational agency or institution to select the proper balance of physical, technological, and administrative controls to effectively prevent unauthorized access to education records, based on their resources and needs. In order to establish a system driven by physical or technological access controls, a school would generally first determine when a school official has a legitimate educational interest in education records and then determine which physical or technological access controls are necessary to ensure that the official can access only those records. The regulations require a school that uses only administrative controls to ensure that its administrative policy for controlling access to education records is effective and that the school is in compliance with the legitimate educational interest requirement in § 99.31(a)(1)(i)(A). However, the 'reasonable methods' standard applies whether the control is physical, technological, or administrative.*
>
> *The regulations permit the use of a variety of methods to protect education records, in whatever format, from improper access. The Department expects that educational agencies and institutions will generally make appropriate choices in designing records access controls, but the Department reserves the right to evaluate the effectiveness of those efforts in meeting statutory and regulatory requirements.*
>
> *73 Fed. Reg. at 74,817.*

**Better Efforts are Needed within the Educational Sector to Implement Technological Controls**

The pie chart on the previous page reveals that more than half (53%) of the security breaches experienced in the education sector over the past several years have been due to exploitations of system vulnerabilities—failure to implement technological controls that would have prevented network intrusions. Hackers identify and exploit network vulnerabilities to gain access to records systems. In other words, educational institutions need to implement better technological controls to reduce the relatively high incidence of security breach that has occurred over the last several years. Here are some suggested techno- logical controls that may help:

• Configure network systems, firewalls, and software properly and in accordance with best security practices;

• Restrict and control access to authorized and authenticated users through the use of digital certificates or other similar mechanisms, and to ensure accountability, each user should have a unique account or set of access privileges. Note that the "reasonable methods" approach is echoed in the requirement for verifying and authenticating the identity of persons to whom records are disclosed:

> *An educational agency or institution must use reasonable methods to identify and authenticate the identity of parents, students, school officials, and any other parties to whom the agency or institution discloses personally identifiable information from education records.*
>
> 34 C.F.R. § 99.31(c).

• Obtain, install, and regularly update software for all workstations and servers— most software vendors regularly release software fixes ("patches") intended to address security vulnerabilities;

• Harden systems by removing or disabling unnecessary software services and applications;

• Implement intrusion detection systems, network monitoring software, and security assessment tools to detect and deter break- in attempts;

• Encrypt sensitive information to protect it in the event that an intrusion occurs

• Monitor outgoing traffic for leaks of sensitive data; and

• Conduct periodic security tests and occasional network penetration testing.

**What is computer security?**

Computer security ensures the confidentiality, integrity and availability of data-- *Confidentiality* of student records, tests, financial information; *Integrity* of student grades or research data; and *Availability* of resources like email or online databases when they are needed.

Schools may no longer rely on piecemeal information security implementations—comprehensive security and privacy policies, programs, procedures and practices need to be put into place. An information security program should consist of physical, administrative, procedural and technical safeguards that mitigate identified risks.

**Physical controls** are locks on doors that protect laptops and network hardware.

**Administrative controls** consist of procedures and practices to address hiring, firing and training procedures that an organization implements to address the human factor.

**Procedural safeguards** are the data handling steps followed to ensure the protection of data as it is processed by the institution.

**Technical controls** are the software and equipment implemented to control the movement of data within the organization's networks.

All of these safeguards or controls protect the institution from perceived threats and vulnerabilities—whether they are external threats (hackers, malware) or even internal (a disgruntled employee, user error or simple negligence).





DigiCert, Inc.
355 South 520 West
Canopy Building II
Lindon, UT 84042
+1-800-896-7973 ph
www.digicert.com

# Benefits of Adopting PKI-based Identity Management

**PKI-Based Security Solutions Implemented in Higher Education**

Historically, access to a variety of educational computing systems has been managed independently (often based on different technologies), by each system. Today, with a wider variety of electronic resources available on campus, this approach is no longer convenient nor is it efficient for users of educational computing systems. Regulatory compliance with FERPA, HIPAA, GLBA, CALEA, etc., necessitate a centrally-based identity management system.

The most commonly implemented user authentication systems on campuses utilize username/password technology. While these are generally easy to provision, they come with a host of administrative disadvantages when access to multiple resources are controlled via this method. If users seek to have a single password for multiple accounts, then synchronizing passwords can become a nightmare not only for the user, but also for system administrators. A single password also creates a single point of failure, meaning every system accessed by that credential is at risk due to the security of the weakest of all the systems – this is problematic for enterprises when individuals reuse the same password for systems outside of the system, e.g. for social networking sites such as Hotmail, Facebook, and Twitter. Another issue with username/passwords in general is that the applications being accessed also need to know the user's password so they can verify it – this creates a single point of focus for attackers, i.e. if an attacker can compromise the password database of the system, they have access to ALL user accounts.

Having multiple passwords, however, becomes too burdensome for users. They start using "easy- to-remember" or weak passwords, or they forget passwords and put further strain on administrators with a higher incidence of password resets. If strong passwords are used, then typically they are recorded and stored locally so they are easy to recall. (Maybe you have seen a note stuck near a computer with someone's password on it.) This makes passwords a weaker option for authentication. A password is a single factor of authentication – it is simply something you know. This makes it easy to share and difficult to revoke. Stronger authentication techniques involve multiple factors of authentication.

There are 3 factors of authentication:

1. Something you know, e.g. a password, image, or PIN
2. Something you have, e.g. a token, smartcard, or key
3. Something you are, e.g. a biometric, fingerprint, or iris pattern

A combination of any two, or all three, of the above—multi-factor authentication--provides a more secure and much stronger binding of the user's identity to the authentication event.

*"While debate continues on what type of technology is best suited to prevent identity theft, many experts believe that a combination of PKI infrastructure and two-factor authentication offers the greatest promise of protection."* Financial Services Technology, Preventing Identity Theft.

DigiCert recommends the use of Public Key Infrastructure, or PKI, which has been part of the computing environment at institutions of higher learning for over a decade. In 1996, the Internet2 consortium, http://middleware.internet2.edu/pkilabs was formed to "facilitate the development, deployment and use of revolutionary Internet technologies." In 1998, EDUCAUSE, http://www.educause.edu/Resources/Browse/PKI/17584 was formed by the merger of Educom and CAUSE, with a goal of "advancing higher education by promoting the intelligent use of information technology." Since their formation, both of these organizations and their members have implemented and promoted the creative use of PKI to meet these stated goals.

Various colleges and universities have integrated PKI into their identity management and authentication systems, including but not limited to Dartmouth College http://www.cs.dartmouth.edu/~pkilab/; University of Virginia; University of Wisconsin; Massachusetts Institute of Technology; and the University of Alabama.

The InCommon Federation, http://www.incommonfederation.org/, uses PKI as the backbone to protect the server infrastructure for Shibboleth http://shibboleth.internet2.edu/, and a SAML- based authentication solution.

**Additional PKI Points**

A PKI-based credential management system can provide:

• Increased security—PKI-based credentials are more secure than password-based access control systems;

• A 1024-bit certificate is stronger than a 128-character password;

• No secret is shared across a network, and is not stored or required at the server side, so there is no single point of focus for attackers;

•Using a PIN to protect the certificate's associated private key is 2-factor authentication, which is far stronger than single factor, and is required in certain contexts by various legislation and regulations;

• A single certificate can easily be managed across multiple systems, and does not suffer from the same synchronization issues as passwords;

• Certificates can be revoked and replaced relatively easily if compromised or delegation rights need to change;

• Cost savings due to centralized management and economies of scale—networks and applications use the same authentication and access granting components;

• Compliance with contracts and IP licensing arrangements—access to course resources and library assets in electronic form are restricted to authorized students and faculty; and

•Cross-certification trust is being created among education, industry and government agencies through arrangements among the Federal Bridge Certificate Authority, the Higher Education Bridge Certificate Authority, SAFE and CertiPath— i.e. the Four Bridge Forum (4BF).





DigiCert, Inc.
355 South 520 West
Canopy Building II
Lindon, UT 84042
+1-800-896-7973 ph
www.digicert.com

# Responsibility and Accountability

**Who has responsibility for information security?**

The organization should designate a specific individual or group of individuals with the responsibility for the development, coordination and implementation of the security program. Is this person the Director of Information Technology or is the group the Office of Internal Audit and Risk Management? What roles do webmasters and security guards play? Do "data custodians" play an active role in establishing security policies? Does information security play a role or have a part in the senior administration of the institution? Do the size of your organization and the tasks required to keep your organization secure merit a full- time or part-time position? Is there a budget allocation for computer security? Does your school have an implementation plan or long- term strategy to improve its security posture? Are there user groups who can facilitate communication of information security messages? Can computer security incidents at peer institutions galvanize support for computer security at your school? These are all important questions to consider.

**Delegate responsibility for information security down to the individual user**

Educate students about good security practices – distribute security guidelines and policies that the institution has adopted. Require all teachers and students to acknowledge and sign an Acceptable Use Policy before their accounts are activated. Also, good user authentication leads to individual accountability, which is the ability to tie an action to an individual. Implement access controls that consist of strong passwords or digital certificates.

Unique user accounts/IDs and passwords should never be shared (except maybe for younger student accounts, e.g. below fourth grade). Students and teachers should also be made aware that violations of security policy will result in a loss of access privileges (and may give rise to other sanctions). Instances of security violations can also be used as teachable moments to improve user behavior. Finally, systems must be able to track who is accessing records in order to comply with the recordkeeping requirements of FERPA.

**Central management of network**

Maintain firewalls and other perimeter devices and software that filter content, block executable attachments from e-mail, and segregate administrative and student networks from each other and the Internet with private IP addresses (or NAT). Manage anti-virus software, stay current with security hot-fixes and patches, and protect machines from malicious software that will turn them into botnets.

**Review policies**

Address policies for administrative computing resources differently than those for academic computing resources so that policies do not unnecessarily inhibit academic activities or academic freedom. Consider integrating computing ethics ("good netizenship") into appropriate parts of the curriculum. Perform due diligence reviews of the privacy and security practices of any third party with whom you share data, and protect against the careless off-site handling of data.

**Additional Security Tips**

**Shop for discounts**. In education, cost will always be an issue because of demands on budgets for salaries, equipment, supplies and many other things. Many vendors—including DigiCert--provide a discount for educational institutions.

**Encryption**. Use encryption and authentication across networks through SSL/TLS Digital Certificates. Require file and disk encryption on sensitive student data.

**Use Strong Passwords**. secret, eight-character password length, known only to the user, with complex syntax such as alpha-numeric and special characters and no simple easy-to-guess passwords or dictionary words.

**Other Reference Sources:**

Information Security in Higher Education: Professional Paper Series # 5, CAUSE, et al., 1991.

IT Security for Higher Education: A Legal Perspective, EDUCAUSE/ Internet2, 2003.

http://counsel.cua.edu/Security/campusecuritybreach.cfm

*DigiCert, Inc. <http://www.digicert.com/> is a leading provider of enterprise-grade, high-assurance, 256-bit SSL Certificates trusted by many national and state governments, educational and medical institutions, and Fortune 500 companies around the world. Located in Lindon, Utah, DigiCert is a WebTrust Certified Certificate Authority and a member of the CA/Browser Forum, the W3C Consortium, the Online Trust Alliance and the Anti-Phishing Working Group (APWG).*

*To obtain DigiCert SSL Certificates, please visit http://www.digicert.com/ssl-certificate.htm*



Press Contact: Travis Tidball - travis@digicert.com



DigiCert, Inc.
355 South 520 West
Canopy Building II
Lindon, UT 84042
+1-800-896-7973 ph
www.digicert.com