

CREDANT Mobile Guardian

Responsible Management of
Endpoint Data Security for Higher Education



The disk is replaceable. The data is not.

Studies show that if you focus on locking down the disk, you're not managing sensitive data appropriately. Instead, you need to quickly deploy security measures that fit your policies for data retention, use and access. The best way to do this is from one central console vs. multiple systems.

Policy enforcement should be automatic yet easy to modify.

IT and Help Desk staff should have the powerful tools to detect data storage devices that need protection, modify policies on existing systems, lock down a stolen or lost device, and make other changes as security needs change.

Threats come from the inside and out.

Most university IT departments begin by providing physical safeguards to restrict data access. But strong yet flexible rules management combined with encryption, and port/application controls will meet threats head on.

Lost laptops are not the only problem.

Your data security system should as easily manage data security on laptops and PCs as it does iPods or other media players, phones, USB sticks, CDs and other disk storage devices.

Strong security and weakened productivity do NOT go hand in hand.

Studies show that users require security to be "easy to use." The trick is to enforce compliance-grade endpoint security that is virtually invisible to the end user.

Flexible reporting is mandatory.

Whether you're meeting legislated audit requirements or your own enforcement tracking, reporting should be accessible via a web-based management console or your chosen system management console.

Secure AND recoverable. Period.

Accidents happen. So having automatic backup of security keys & policies is a must.

COMPLIANCE IS NOT ACADEMIC

According to the 2008 EDUCAUSE Current Issues Committee, the number one strategic IT issue for educational institutions is security.

That's not surprising considering the high profile press coverage on data breaches. Protecting information, particularly on multiple mobile endpoints, is more important than ever. And higher education poses unique challenges in sheer diversity of data, ranging from admissions financial information to campus medical clinic patient records to classified research.

In all cases, encrypting information occurs in a culture of openness and decentralization. IT managers frequently have to deal with encryption schemas that vary from school to school, department to department.

In all cases, regardless of any single legislation or compliance law, there are some basic questions that ensure appropriate handling of data, such as:

- › Are privacy and security policies for encryption regularly reviewed? Consistently implemented?
- › Is there an authority within the university, such as a chief security officer, who can wade through the increasing number of compliance laws?
- › Are audits regularly scheduled and scrupulously implemented?
- › Have you developed clear, consistent policies and procedures for classifying, handling, retaining, and disseminating information and appropriate security controls for protecting critical and confidential resources?
- › If a device, such as a laptop or USB key, be lost or stolen that has data stored on it that falls within a regulation, are there notification methods in place based on the level of security you provide?
- › Is IT security viewed as a funding priority?

These questions and others support a strong data security management framework. And with data security breaches estimated at costing between \$90 and \$305 per lost record, the impact of not addressing these questions can be crippling to universities, colleges and schools of all sizes.

LEGISLATION AND REGULATION

Following is a snapshot of regulations impacting institutes of higher learning today:

Family Educational Rights and Privacy Act (FERPA)

The federal Family Educational Rights and Privacy Act of 1974 (FERPA) provides a postsecondary student the right to inspect his or her education records and establishes conditions concerning the disclosure of those records to third parties. Although the act does not specifically require that information security be implemented, the protection of electronic student records will require information security covering the student records subject to this federal law.

Health Insurance Portability and Accountability Act (HIPAA)

First described in 1996, the final HIPAA standards rules was published in 2003. HIPAA identifies a series of security procedures to assure the confidentiality of electronic health information. These procedures include administrative, techni-

CREDANT Mobile Guardian

Responsible Management of
Endpoint Data Security for Higher Education



CREDANT delivers data security for today's schools, colleges and universities

Automated endpoint data security administration, comprehensive reporting and the ability to quickly implement changes to address today's data at rest security needs are available from CREDANT software.

CREDANT's policy-based Intelligent Encryption provides centrally-managed, highly scalable and architecturally flexible security needed to manage all data endpoints. CREDANT's encryption software protects data on over 4.5 million devices worldwide. More than 650 enterprises and government agencies -- including 50 of the Global 500 -- rely on CREDANT to ensure security compliance, protect their brand and enhance IT and end user productivity. Previous generation technologies simply cannot keep pace with today's wide variety of endpoints where data can be stored.

Only CREDANT Mobile Guardian (CMG) ensures that your security policies are consistently and efficiently enforced -- regardless of where the data resides. To learn more, go to www.credant.com.

cal and physical measures. In the higher education arena, HIPAA most often applies to clinics used by both students and staff and to academic medical centers. Along with detailed security rules, HIPAA includes provisions to investigate complaints, collect information and determine a covered entity's compliance.

FDA Rule on Electronic Records and Electronic Signatures (21 C.F.R. Part 11)

In 1997, the U.S. Food and Drug Administration (FDA) issued 21 C.F.R. Part 11, which consists of regulations that provide criteria for the acceptance of electronic records. These criteria include specific information security and electronic signature practices. Part 11 applies to electronic records transmitted under any FDA regulations or submitted to the FDA. Therefore, it applies to most aspects of research and clinical activities in the university setting. Key provisions, such as controls of "open systems" such as portable data devices to limit access have been added. Audit controls, password protection and backup provisions are also requirements.

Gramm-Leach-Bliley Act (GLBA)

Under GLBA, the Federal Trade Commission (FTC) has jurisdiction over the activities of higher education institutions. The FTC regulations contain both privacy and security requirements. Colleges and universities that comply with FERPA will be deemed by the FTC to be in compliance with its privacy provisions. However, educational institutions remain subject to the GLBA security provisions as found in the FTC safeguard regulations ("FTC Safeguards"), which became effective on May 23, 2003.

The California Law on Notification of Security Breach (SB 1386)

The California Law on Notification of Security Breach (SB 1386) relates more to disclosing a security breach vs. the security of the data itself. Notification could be delayed if there is a legitimate law enforcement agency determined that giving notice to the data subject would impede a criminal investigation. Notice may also be delayed if the organization suffering the breach is taking necessary measures to determine the scope of the breach and restore reasonable integrity to the system. Over 30 States have passed similar legislation.

The Payment Card Industry Data Security Standard (PCIDSS)

If your admissions office takes credit cards for payment, then you is subject to the Payment Card Industry Data Security Standard (PCIDSS). The PCIDSS requires that all "merchants" accepting credit cards comply with a number of technical, physical, and administrative requirements. Failure to comply with the PCIDSS could result in large penalties and suspension of the right to use credit cards for payment purposes.