Compliance Scorecard

Security Leadership Solutions Executive Council

FERPA Compliance

Protecting student records through due diligence

By Jon L. Oliver

Compliance means never having to say you're sorry — sorry the network was hacked, sorry the access control system wasn't properly maintained, sorry for the privacy breach or loss of assets. Compliance is not a technology or a magic bullet — it is simply a way of doing business that allows your legal department to go home at a reasonable hour.

While higher education has been somewhat immune to the legislative frenzy, those of us who work in the field should look around at other highly regulated areas and take a lesson: It is much better to be proactive, knowing that your institution is thinking ahead to protect assets, people and information, than to be the test case in the courts later on. The lawyers call this "due diligence." Sometimes even when legislation is in place, it takes due diligence to ensure that your institution is complying with both the letter and spirit of the law.

In short, the role of FERPA is to ensure that private student records are not disclosed to anyone without the consent of the parent until the student reaches the age of 18, when the right is transferred to him or her.

One overarching regulation that applies to higher education is the Family Educational Rights and Privacy Act (FERPA). Enacted in 1974, it has been amended 28 times. In short, the role of FERPA is to ensure that private student records are not disclosed to anyone without the consent of the parent until the student reaches the age of 18, when the right is transferred to him or her. Private records include transcripts, exams, enrollments, disciplinary actions and health records.

Much of this data is held in centralized databases run by IT professionals who securely maintain it; however, much more is still potentially resident on faculty systems with few, if any, safeguards. When users are in control, as in this case, certain problems will surely arise:

1. Users will lose data. They may delete files unintentionally or lose their laptop in the airport or by theft. No electronic data is absolutely safe. This is because what once required reams of paper that could be monitored and accounted for can now fit into a small USB drive that fits into your pocket and just as easily falls out.

2. Users will keep private data where it should not be kept. I have seen Social Security numbers, home addresses and grades posted on the Web.

3. Users will try to hide sensitive information. They think that if they hide information by choosing awkward file names or by burying it a few layers beneath the root or "My Documents" directory, no one could possibly find it. This is known as security by obscurity. It is also, of course, a fallacy.

4. When confronted with the need to protect information, users will want to do it, but won't know how. IT professionals can add the latest security technologies, but if they are not used properly, the end-result is worse than if no protective mechanism were used at all. This is because the illusion of protection confers some false sense of security and can lull the user into believing that all is well when it is not.

For any protective measure or policy to be effective, it must be firmly ingrained in the very psyche of the user. It should not be difficult or complicated, and it cannot require any action beyond the press of a button.

Based on these truths, we can offer a few simple ideas to follow to ensure that you are complying with both the letter and spirit of FERPA:

- Don't keep any private student data on any machine not centrally controlled and secured by professionals with a strong security background.
- Look at every bit and byte of data on all your faculty and staff systems and assess whether you truly need it there. There is nothing worse than unnecessarily storing data in multiple places only to find out later that it was unprotected, and that you now must disclose a security breach.
- If you ignore numbers 1 and 2, at least encrypt your hard drive and secure user machines with strong passwords and tokens.
- Disclose your responsibilities and those of your faculty and staff at least once a year as a reminder to keep security, privacy and confidentiality at the front of everyone's mind. STD

Jon L. Oliver is assistant dean and director of information technology for the School of Communication, Information and Library Studies at Rutgers University, an educational partner of the Security Executive Council. The Security Executive Council maintains a large and growing list of laws, regulations, standards and guidelines that impact security (https://www.securityexecutivecouncil.com/public/lrvc). For more information, visit www.SecurityExecutiveCouncil.com/?sourceCode=std.