

Simplifying Compliance with FERPA Rules



October 2010

FERPA Privacy Rules: Setting security standards for education institutions

The Family Educational Rights and Privacy Act (FERPA)¹, most recently amended in 2008, has raised the bar of security for educational institutions.

New standards have been put in place to protect students' personal information, education history and data. Schools, universities and other educational institutions need to ensure the rules are followed within their business associates' organizations, such as outsourcing companies.

FERPA includes administrative and technical requirements around many aspects of students' lives and data. Among those, FERPA requires educational institutions to ensure:

- Students' personal data are not disclosed without prior written consent
- Access to students' records is only allowed to individuals with well defined reasons to be in need to accessing the information

Access control and data protection are requirements for compliance

At a very high level, Section 99 of FERPA requires the adoption of comprehensive security measures that include access control and data protection solutions.

For example, Section 99.30, stating "[...] The parent or eligible student shall provide a signed and dated written consent before an educational agency or institution discloses personally identifiable information from the student's education records [...]", may imply that educational institutions are

responsible if students' information is lost or potentially disclosed to unknown individuals such as a teacher losing his laptop with students' grades.

Similarly, Section 99.31(c) states that institutions should use "[...] reasonable methods to identify and authenticate the identity of [...] any party to whom the agency or institution discloses personally identifiable information from education records." Section 99.31(a)(1)(ii) also notes that, if technological access control solutions are not in place, the institution has to bear the burden of ensuring internal processes provide an adequate level of security and protection².

FERPA compliance with DigitalPersona® Pro

DigitalPersona Pro provides businesses of all sizes with a powerful, flexible solution for preventing unauthorized access to data and computer systems.

DigitalPersona Pro provides efficient management of multiple security and authentication applications, simplifying education providers' efforts to achieve security and compliance. In addition, its low Total Cost of Ownership (TCO) and compatibility with existing infrastructure enable schools to boost the return on investment of their existing systems.

The following examples show how DigitalPersona Pro can assist your school with FERPA requirements.

The screen images shown are from DigitalPersona Pro Enterprise, which provides Active Directory based management of security and authentication policies to businesses of any size. Most of the capabilities in DigitalPersona Pro Enterprise are also available in DigitalPersona Pro Workgroup, which provides easy-to-manage, affordable out-of-the-box security for

¹ Family Educational Rights and Privacy Act (FERPA), Final Rule, 34 CFR Part 99, Section-by-Section Analysis, December 2008.

² Id. at 1.

small businesses and departments within larger organizations.

Example 1. Compliance with FERPA 99.30 et seq.: Information disclosure

As previously mentioned, FERPA 99.30 requires institutions to receive written consent from students or students' families before disclosing sensitive information³. As a result, FERPA 99.30 de facto introduces the need for educational institutions to protect data at rest whenever stored in locations or devices that might lead to accidental loss, such as lost or stolen laptops. Many institutions have adopted or are considering the adoption of measures like Full Disk Encryption to prevent accidental data losses from happening.

DigitalPersona Pro can help meet the requirements imposed by FERPA 99.30 by providing several security methods to protect data stored on a computer.

With DigitalPersona Pro, IT Managers can enforce encryption of the entire hard drive on managed computers.

Once the hard drive is encrypted, users will be required to provide proper authentication credentials (password, fingerprint, or smart card), according to policies specified by the IT manager, before the Windows operating system starts (i.e. pre-boot authentication).



For convenience, the software provides the option to automatically unlock the drive and securely log on to Windows without further authentication (i.e. so-called Single Sign-On or One-Step Logon).

DigitalPersona Pro's Full Disk Encryption meets the technical requirements mandated by NIST for both data at rest and data in motion, which include AES algorithm and/or FIPS 140-2.

Example 2. Compliance with FERPA 99.31(c): Authentication of individuals accessing sensitive information

FERPA 99.31(c) requires institutions to "[...] use reasonable methods to identify and authenticate the identity of [...] any parties to whom the agency or institution discloses personally identifiable information [...]"⁴. Within an institution's organization, typical cases of problematic situations that may cause breaches include users sharing credentials to log on to computers or applications.

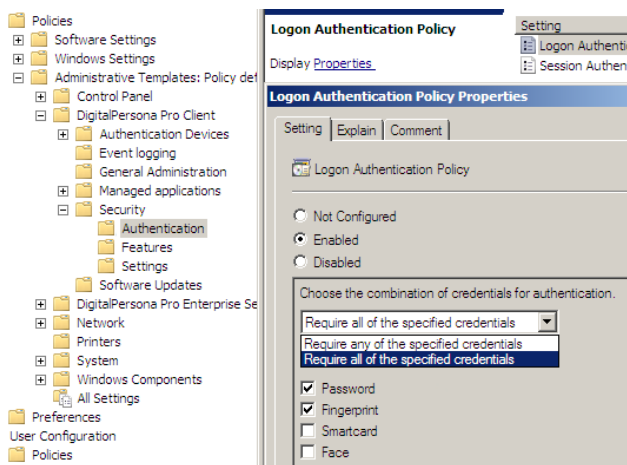
DigitalPersona Pro supports strong authentication which helps IT Managers meet the requirements imposed by FERPA 99.31(c). Two-factor authentication, including biometrics, makes it more difficult for users to share credentials, thus reducing the risk of unauthorized access. DigitalPersona Pro also supports shared workstations and kiosks.

³ Id. at 1.

⁴ Id. at 1.

With DigitalPersona Pro, IT Managers can select and enforce authentication policies for computers and application logon in just a few steps. For example, to mandate a two-factor logon policy requiring a password and a fingerprint, IT Managers can use DigitalPersona Pro Enterprise to:

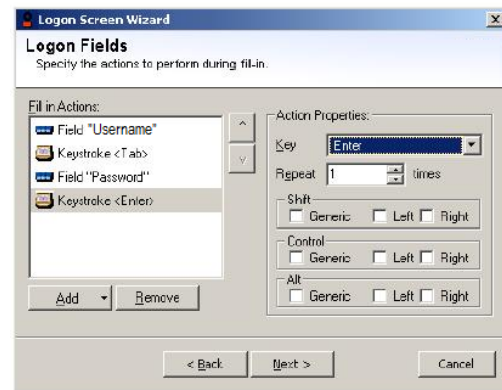
1. Go to the Active Directory **Group Policy Management Editor**
2. Browse to **Computer Configuration > Policies > Administrative Templates > DigitalPersona Pro client > Security > Authentication**
3. Double-click the **Logon policy** policy object
4. Select **Enabled**
5. Select **Require all of the specified credentials**
6. Select **Password** and **Fingerprint**



DigitalPersona Pro can also help meet the requirements imposed by FERPA 99.31(c) by allowing IT Managers to configure password management and single sign-on to all enterprise applications. IT Managers may even want to randomize passwords, or not let users know their own passwords, thus making it impossible to share credentials.

With DigitalPersona Pro Enterprise, IT Managers set up application logons through a simple wizard. Setup

only takes a couple of minutes per application and requires no changes to the existing application. Support extends to virtually all applications, including Citrix, Web apps, Windows and terminal applications.



IT Managers can also choose to configure authentication policies for managed applications to require no credentials (i.e. Single Sign-On) or any combination of passwords, smart cards and biometrics, such as fingerprints.

Once the logon is configured, IT Managers can deploy this information to managed workstations through Active Directory Group Policy Objects.

To Learn More

For more information about DigitalPersona Pro, visit www.digitalpersona.com/pro or contact us at:

- Email: sales@digitalpersona.com
- In North America, call: +1-650-474-4000
- In EMEA, call: +44-203-286-4004

Free trials are also available.

About DigitalPersona

DigitalPersona, Inc. is a global provider of authentication and endpoint protection solutions that

make security simple, practical and affordable for businesses of all sizes. The company helps enterprises, government agencies, custom application developers and independent software vendors to efficiently address growing security, compliance and fraud-prevention demands. DigitalPersona's award-winning technology is offered by market-leading computer manufacturers and solution providers around the world.

Disclaimer

THE INFORMATION IN THIS DOCUMENT IS PROVIDED FOR INFORMATIONAL PURPOSES ONLY AND IS NOT INTENDED TO BE ANYTHING OTHER THAN THE EDUCATED OPINION OF THE AUTHOR. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS DOCUMENT ARE BELIEVED TO BE ACCURATE BUT DIGITALPERSONA MAKES NO CLAIMS, PROMISES OR GUARANTEES ABOUT THE ACCURACY, COMPLETENESS, OR ADEQUACY OF THE INFORMATION. THIS INFORMATION SHOULD NOT BE RELIED UPON AS LEGAL ADVICE. DIGITALPERSONA SPECIFICALLY DISCLAIMS ALL WARRANTIES OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS OR COMPLIANCE WITH ANY LEGAL REQUIREMENTS.

© 2010 DigitalPersona, Inc. All rights reserved. DigitalPersona is a trademark of DigitalPersona, Inc. registered in the U.S. and other countries. All other brand and product names are trademarks or registered trademarks of their respective owners.