

Design of FERPA Data Integrity

Donald Moss

Strayer Moss

Information Technical Audit & Control

Professor Daniel C Doe

Design of FERPA Data Integrity

US Congress enacted the Family Educational Rights and Privacy Act (FERPA) which allows student parents access their children's records. This act also bans other third parties from accessing the records. To preserve data integrity in the student records system, there are a multitude of techniques to make sure that the technical safeguards are observed for FERPA (Gur, 2018). The latest technological advancement has seen the use of the network storage and new technological trends that has led to easier access to files and efficiency. Technology has made it easier, but there have also been additional challenges that have come up and there is a need to re-design FERPA Technical Safeguards.

Physical access control safeguards

It is important to note that physical access control mechanisms entail who access the records, where, and when. In other words, physical access control involves creating a barrier to prevent unauthorized people from accessing certain information and allowing the right people to access the data. One of the key methods of upholding data integrity is through proper ways of locking server room doors and effective protocols of permitting people to enter the room (Hirschfeld & Cation, 2011). This restricts unknown people from wandering into the server rooms and also accessing important materials and equipment. Categorically, there are two measures where physical access control should be safeguarded; traditional measures that involve the use of locks, constructing perimeter to protect network resources, and digital measures. Digital-based security measures entail the use of fingerprints, the use of closed-circuit television (CCTV), passwords, and digital cards.

Some of the important recommendations include the use of an intrusion detection system that would monitor the network traffic detect anomalies and generate alerts appropriately

(Javaid et al., 2016). In particular, for the student records, a network intrusion detection system should be installed. This is deployed in strategic positions of the network. Probably, the network intrusion system will track inbound and outbound traffic to and from all devices accessing the resources in the server. Registrar's office could even upgrade and make use of an active intrusion detection system called intrusion detection and prevention system.

Not only will intrusion detection and prevention systems generate warnings but also configured to take effective action against intruders. Such actions include blocking IP addresses and shutting down protected resources. Thus, the intrusion system comes with greater benefits including providing the registrar's office greater security visibility, easier identification of vulnerabilities, and enhanced responses.

Deployment of cloud computing is another vital recommendation the institution can put into consideration. Although proper techniques of physical access control might be used there is a chance that the integrity of the student records could be compromised. Cloud computing is the solution. The use of cloud computing by the institution would lead to transformative impacts (Hayes, 2013). Things and equipment that posed security hazardous will be moved to the cloud. The institution will get rid of protecting the hardware and other equipment. All the student records will be accessed virtually through the internet. A lot of advantages are likely to accrue with the use of cloud computing. For instance, users allowed to access the records are able to access anytime and anywhere.

Proper audit controls in the registrar's office.

I could recommend the registrar's office to develop and maintain IT procedures and policies, constantly review IT standards and ensure documentation of every IT resource are kept, observe and interview all data custodians and examine if the registrar's office meets the expected performance.

Three logical access control

There are ways of ensuring that consumers are able to recognize and authenticate themselves, while having the rights to access particular properties (Srinivasa & Viswanathan, 2013). Proof of identity, validation, and authorization are all specific to the safety of IT resources. There are three logical access control methods that are used to restrict unauthorized entries from the sensitive data including account restriction, passwords, and group policies. I would set up account restriction first, because it would limit data users from accessing student records during specific times (Javaid et al., 2016). Administrators would be able to access the accounts and adjust the accounts during specific time periods only. During these time frames, administrators can observe and manage what goes on in the system. Accounts not in use are terminated so it is likely to decrease hackers from performing malevolent undertakings.

The second method I would implement is the use of strong passwords. Users should create and keep strong names and passwords at all times. By doing this, hackers have a harder time accessing student records. Another fundamental access is group policy, which is a set of policies on accessing sensitive data. Policies and protocols apply and automatically place restrictions. These policies are implemented to allow only specific individuals to enter the records and then deny others.

Movement of data in the organization and transmission security

It is the duty of the owner to keep the data confidential. To keep the data safeguarded, it is especially important to know how the data is being moved from one person to another. The data administrators should follow rules and procedures while protecting the records. Data

users should adhere to the stipulated ways of accessing the data. Both parties have responsibilities in protecting data.

Evolving and planning FERPA Safeguards in the record-keeper's office certifies that records are safe and opened by the right people. This ultimately concludes proficiency, precision, and uniformity inside the division.

References

Hayes, B. (2013). Cloud computing.

Hirschfeld, R. A., & Cation, M. K. (2011). U.S. Patent No. 8,009,013. Washington, DC: U.S. Patent and Trademark Office.

Gür, T. M. (2018). Review of electrical energy storage technologies, materials and systems: challenges and prospects for large-scale grid storage. *Energy & Environmental Science*, 11(10), 2696-2767.

Javaid, A., Niyaz, Q., Sun, W., & Alam, M. (2016, May). A deep learning approach for network intrusion detection system. In *Proceedings of the 9th EAI International Conference on Bio-inspired Information and Communications Technologies (formerly BIONETICS)* (pp. 21-26).

Srinivasa, S. M., & Viswanathan, V. (2013). U.S. Patent No. 8,443,437. Washington, DC: U.S. Patent and Trademark Office.