ALLEN SCHOOL
est.1961
of Health Sciences

"Where Education Comes To Life"

Data Security

Policy:

The Allen School of Health Sciences is committed to maintain the highest standards for the safety and security of our students. Under the Student Aid Internet Gateway (SAIG), Program Participation Agreement (PPA), and the Gramm-Leach-Bliley Act (15 U.S. Code § 6801), the Allen School of Health Sciences is required to protect our student personal information, and support our staff in the security of administering the Title IV Federal student financial aid programs authorized under Title IV of the Higher Education Act, as amended (the HEA).

Cybersecurity Process:

Allen School of Health Sciences takes precautions to protect our students' information when submitting sensitive information electronically.

Only employees who need this information to perform a specific job are granted access to personally identifiable information.

i. Information is provided to IT Department (Solarus) with detailed information of the users data requirements
ii. Employees no longer working for the Allen School of Health Sciences has all user rights terminated (Immediate notification is send to Solarus and all vendors to request termination).

Allen School of Health sciences computers/servers in which we store personally identifiable information are kept in a secure environment.

I. Confidentiality is achieved using NTFS and Share permissions control access to folders specified as confidential. Folders/files that Allen School of Health Sciences deems confidential are locked down to specific users/groups. Allen School of Health Sciences users would be using email encryption for anything sensitive sent over email. Allen School would have to determine integrity, whether data is accurate and trustworthy. Availability of server data is mitigated by performing routine backups with a disaster recovery plan to have data available if physical server goes down.
II. Firewalls also have content filtering enabled, restricting users from accessing categories of sites, as well as blocking malware sites. DNS is set to forward to OPENDNS, to provide another layer of protection.

Workstations and servers have centrally managed Antivirus, as well as centrally managed Malware Bytes as a second layer of defense. Other second opinion scanners are run weekly to identify anything that the other products may have not identified. Email is provided by google gsuite, with Google providing a layer of email security.

The first step is to identify the virus/hack, then review logs and identify how the systems were attacked. Review infected system running processes. Using centrally managed security products, a sweep would be performed on all machines. Any infected machines are assessed. If not able to identify the attack, machine would be pulled off the network. A security response consultant will be called when necessary to remove hardware.
Hardware/Software Data Security Protection Includes:

- Firewalls
- Access control list (ACL) on all border routers
- Intrusion detection system (IDS)/intrusion prevention system (IPS)
- Virtual local area networks (VLANs)
- Email encryption
- Secure file transfer
- Secure printing
- Safe recipient email list
- Data loss prevention (DLP) on all endpoints CLOUD
- Encryption of data on servers
- Hard drive encryption
- Internet proxy with malware, antivirus and DLP protection

Vendors used by Allen School of Health Science are required to have and implement security measures in place to protect the information of our students.

ECMC and CVUE Management has developed and implemented an enterprise-wide shared service information and physical security program that is designed to ensure the security and confidentiality of borrower records and information, protects against anticipated threats to the security and integrity of the records and protects against unauthorized access to or use of such records or information. The program utilizes security framework and in accordance with vendors security policies, the information security program contains administrative, physical and technical safeguards to protect borrowers' non-public personal information.

Allen School of Health Sciences Employee management and training

Allen School of Health Sciences has the department of Human Resources supply information and training to new employees upon the hiring process.

Every July 1st the Allen School of Health Sciences sends a power point presentation to all faculty and staff with information on Data Security best practices.

Students upon enrollment receive the Allen School policies and procedures Data Security as part of our Annual Consumer information electronically.