Genesis Educational Services System Policy

The purpose of this policy is to maintain an adequate level of security to protect data and information systems from unauthorized access. This policy defines the rules necessary to achieve this protection and to ensure a secure and reliable operation of information systems.

1. This policy affects all employees of Genesis Educational Services. Employees who deliberately violate this policy will be subject disciplinary action up to and including termination.

Only authorized Genesis Employees are granted access to Genesis systems. System access control is to be achieved via unique user IDs and MFA (multi factor authentication) which are to provide individual accountability.

1. All employees must be screened prior to hire.
2. Employees are required to attend informational security awareness training.
3. Policies in place requiring HR to immediately notify IT of terminations and transfers.
4. All Genesis employee system actions will be logged and stored indefinitely.
5. Genesis does not allow ANY 3rd party vendor ASP/hosted system access.
6. Procedures for access to mission critical systems and sensitive data include user authorization and authentication protected by MFA (multi factor authentication).

Hosted Internet environment security

- Internet accessible systems are tested for vulnerabilities prior to being placed in production.
- Only services that are required by a specific business need and that have been assessed for their impact on security are enabled.
- All essential protocols are securely configured, and non-essential protocols are disabled.
- Firewall(s) are configured to ensure source(s), destination(s) and protocol(s) are as specific as possible.
- No internal systems containing client information or in the same network are exposed directly to the internet.
- External networks and DMZ servers are monitored for security violations.

Internal system security

- Applications on internal web servers run in non-privileged mode.
- Server performance metrics (CPU, disk, memory, hardware, etc.) are monitored.
- Genesis ASP network (managed by Cologix) protected by firewall with IPS (Intrusion Prevention System), DDOS protection, antivirus and DLP (Data Leak Prevention).

Critical systems receive full security testing before deployment

- Attack and penetration testing is performed internally.
- Testing for web applications includes checking for session management weaknesses, cross-site scripting, SQL injection and other vulnerabilities.
- Application is tested twice annually.

Encryption

- Public/private keys are used for the encryption of sensitive information during transmission.
- SSL TLSv1 or higher is required for data going over public networks.
- There is a secure email capability.
- Passwords are a hash+salt.
- Full disk encryption is used for locally stored materials (e.g. on laptops, workstations, etc.)
- Encryption keys are securely controlled.

Genesis ASP infrastructure is housed in a Cologix Data Center which maintains strict physical controls. Specific controls listed below are in place at the physical server location. (www.cologix.com)

- A security perimeter has been identified and documented, which includes computer rooms, media storage rooms, data centers, etc.
- Biometric access controls are used to access company data center(s).
- Computers are physically secured with lock devices.
- Surveillance cameras and security officers are in place to monitor premises.
- Departments and work areas that deal with sensitive information or systems are limited to authorized personnel.
- ID badges are required for employee access.
- ID badges are electronically verified for access.
- Activity logs are periodically reviewed for suspicious access.
- Computer, media storage and telecom room access is secured and restricted to authorized personnel.
- Cables and network ports are protected from unauthorized access.
- Disposal of computer systems and media storage devices (hard drives, tapes, floppies, CDs, etc) is handled in a secure fashion (i.e. de-magnetization and/or destruction).
- Remote locations have physical security similar to the main location.
- Physical access control is managed similar to the logical access control process, i.e. authorizations, role-based access, rapid termination, and regular reviews of entitlements.
- Use of key bypass to badge access is strictly monitored and keys are managed similar to the logical access control process.

System logs are maintained for the following (Physical access is managed by Cologix):

- Internet connections
- Critical applications functions
- Facility access and surveillance
- Use of privileged system functionality
- Logs are stored securely in a central location

Data center logs are available upon request via NDA.

Genesis Data Backup Service infrastructure is housed in AWS S3 which maintains strict access controls. Some specific controls listed below are in place. Additional information can be found in the S3 user guide.
(https://docs.aws.amazon.com/AmazonS3/latest/userguide/s3-compliance.html)

- AWS Identity and Access Management (IAM)
- AWS Key Management Service (KMS)
- Supported frameworks such as CIS, ISO, SOC, PCI-DSS, and NIST