ENTOURAGE INSTITUTE
of Beauty & Esthetics

Gramm-Leach-Billey Act
Student Information Policy

Entourage Institute of Beauty and Esthetics Student Information Policy is in place to ensure that the school protocols to ensure student information integrity and security is in place with regards, to data, email, financial and internet security within the campus environment. Entourage Institute has adopted a robust plan to ensure that all student information is secure and is not able to be accessed by outside sources and compromise both Student and the School's information.

Entourage Institute of Beauty and Esthetics has put in place protocols and software to network integrity of the campus. This includes the following:

- Multi-factor authentication for all administrative work stations, and student information systems within the campus.
- Provide a layered defense. Of Proofpoint, Microsoft 365 email security, Vipre Endpoint Protection, Fortinet Firewalls with Layer 7 Security features
- Secure Configurations – Airespring and IT support contractor Rocketman Technology ensure that all network equipment is secure and tested before installation. This is required prior to any hardware being added to the system.
- Access control – Sensitive data is maintained within OneDrive and Fame Student Information System, with no external server availability. Only Entourage Institute of Beauty and Esthetics staff and management may access the company OneDrive system with security levels set for access to different data.
- Firewalls and Intrusion Detection/Prevention Systems – This is provided by Airespring with a Fortinet Firewalls with Layer 7 security systems.
- Patch Management – Vipre Endpoint Protection is installed on all workstations to ensure patch management is in place.
- It is the policy of Entourage Institute of Beauty and Esthetics to not email or receive any PII or other Sensitive data through email. Data is delivered through encryption software with Exchange Online or through our secure Dropbox.
- The Compliance Office and Rocketman Technology are notified of any incidents that may contain breach of sensitive data. Entourage Institute of Beauty and Esthetics works in conjunction with our security providers, (Vipre, Airespring, Proofpoint, and Rocketman Technology) to immediately address and react with appropriate steps to correct the issue.

- Scans are ongoing through the systems and notifications sent to Spencer Reno, with business office, and Rebecca Clothier, Compliance officer for review of potential issues. In addition, weekly a complete scan of all systems and resolution of any notifications is completed by the campus (Spencer Reno) with appropriate steps taken if there is notification of an issue.
- Annually, Entourage Institute of Beauty and Esthetics does a review of the security policy and software in conjunction with Rocketman Technology to ensure that any updates, to the policy is taken into advisement.
-

IT Control Matrix

Potential Risk	Response (How is the risk mitigated?)
Unauthorized access to data that may result in improper changes to, or deletion of data, unauthorized changes to data in master files, or unauthorized changes to IT applications or other aspects of the IT environment.	All software used is password protected and security levels have been set per job requirements. 3rd Party (Microsoft) Identity Authenticators are implemented for sign in to applicable software.
IT personnel gaining inappropriate access to data beyond their assigned duties, inappropriate manual intervention, or other segregation of duties issues.	Shared files in Microsoft OneDrive are limited to those who are in need of access. (not widely shared amongst all staff)
Firewall is in place with Aire Spring which monitors and maintains	Only authorized personnel – Spencer Reno, and Rebecca Clothier – may input tickets to Aire Spring for Firewall opening to outside sources for software Maintenance that may be needed. Access is monitored and closed immediately upon update that may need to be done. Aire Spring constantly monitors and maintains Firewall of systems.
Failure to make necessary changes to IT applications or other aspects of the IT environment.	All 3rd party applications used for Authentication, Malware protection software, etc. such as Viper and Microsoft are server hosted and have auto update functions to keep device applications and software up to date. Firewall through Aire Spring has to grant access to network.
Potential loss of data or loss of access to data as required.	Data is stored on cloud based servers with One Drive that has data backups and recovery in the event of data loss.
Computer hardware, such as file servers, that are storing financial application data are maintained in a secure location and that access to them is restricted to only authorized personnel.	No file servers are currently in use. All financial aid applications are housed are housed with FAME Financial Aid Software which is a Remoted Desktop Application which is maintained by FAME and requires 3rd Party –

	Microsoft Identity Authenticators and is assigned through FAME
The entity performs routine backups of its financial systems and information.	Entourage contracts with Rocket Technology which maintains IT software and systems. Ongoing Internal Review is maintained and review by Spencer Reno, Business Office Administrator, and Rebecca Clothier, Compliance Officer with daily review and monitoring through Proofpoint essentials notification of Quarantine items for review. Any issue that may need greater scrutiny is escalated to Rocket Technology for assistance. Rocket also does ongoing monitoring to ensure that systems is secure and any quarantined items that has not been reviewed is noted to Entourage
Frequency?	Daily
Location?	Lenexa, KS & Lincoln, NE
Access restricted to authorized personnel?	Yes – only Rocketman Technology has access and all additions to software systems in computers or changes to computers has to have administrative password capability which is restricted to Rebecca Clothier and Spencer Reno
Tested periodically?	Yes - quarterly