Keune Academy by 124 - Information Security Program

Introduction Security Program

June 9, 2023

Keune Academy by 124
755 Lawrenceville Suwanee Rd
Bldg 1300,
Lawrenceville, GA 30043

In keeping with the Federal Trade Commission (FTC) regulations (Final Rule) to amend the Standards for Safeguarding Customer Information (Safeguards Rule), an important component of the Gramm-Leach-Bliley Act's (GLBA) requirements for protecting the privacy and personal information of consumers, Keune Academy by 124 (K124) partners with RELITEK Solutions, Inc. to manage all their IT services and cybersecurity practices.

This document is a step-by-step reasonable information security program that identifies the nine elements of the Safeguard Rules.

Designation of Qualified Service Provider

RELITEK Solutions, Inc. has been designated as the qualified service provider for K124. RELITEK has been in business since 2007 and has partnered with K124 to provide IT Managed Services since 2009. John Bowles is the consulting engineer that will be responsible for ensuring the entire environment is secure and is the author of this document.

RELITEK Solutions, Inc.
CEO\Lead Engineer
johnb@reliteksolutions.com
678-344-7481

Risk Assessment

Keune Academy by 124 conducts computer-based business in two different offices. All details related to the security of both internal LAN and external WAN access controls is depicted in this document. The goal is to not only document where K124 stands as it relates to cyber security but to formulate on ongoing plan to protect all student\customer information.

Customer Information – Risk Assessment

A high-level inventory is depicted below under the Inventory Data section. All student\customer information is stored mainly on our main server in the Grayson headquarter location in our main program called Fame. All employees that access this data do so through several avenues such as an encrypted site-to-site VPN or client VPN connection.

Safeguards Rule

In order to provide ongoing controls related to our Risk Assessment we have listed eight safeguards that will ensure our Risk Assessment is not only constantly up to date but also tested.

Access Controls

Out of all the employees, listed in this document, only specific employees have access to student\customer information. The general manager of K124 keeps track of each employees access.

Inventory Data & System

The only location that critical information is stored is the server at the main office in Grayson.

Main Office – Grayson, GA

This facility is the corporate main office for the entire company. The following components cover the Network at that location:

- ISP – Comcast
- Firewall – SonicWALL TZ370
  - VPN Point-to-Point connection to K124 school
- 1 Subnet
- 10 computers
- Antivirus and Website scanning: Webroot and Webroot DNS is a cloud based antivirus program installed on every device on the network.
- Netgear 48-port switch
- Wireless – Netgear WAX630
- 2 physical HP ML350 ProLiant Servers running Windows Server 2016
  - Server #1 Roles: Domain Controller, File, Application
    - FAME Software: main database for all student\customer data.
  - Server #2 Roles: Domain Controller, DNS, DHCP, Application
- 1 Hyper Windows Server 2016
  - Virtual Server Roles: Remote Desktop access, File and print

School Facility – Lawrenceville, GA

This facility is the main location where the classrooms are located and staff is housed. The following components cover the Network at that location:

- ISP – Spectrum
- Firewall – SonicWALL TZ470
  - VPN Point-to-Point connection to main office
- 1 Subnet
- 11 computers
  - 6 Laptops: Sonicwall Netexternder VPN to connect to the main office when users are remote.

- Antivirus and Website scanning: Webroot and Webroot DNS is a cloud based antivirus program installed on every device on the network.
- Netgear 48-port switch
- Wireless – NetGear WAX630 Access Points
- Public Wireless on separate subnet

The list of end users listed below. Only 6 of them use the NetExtender Sonicwall VPN to connect when at home or out of the office:

- Anna Dill
- Arihanna Douglas
- Angel Hampton
- Alan VanHassel
- Ashleigh Williams
- Chris Hinton
- Carrie Pressley
- Cory Self
- Elizabeth Groff
- Kim Kibble
- Krystal Self
- Lauren McGuire
- Masi Arellano
- Melody Jaggar
- Paige Bessant
- Ojilcri Arias Reyes

Encryption

All customer data is encrypted. First of all, emails that are sent out using Office 365 when a customer's private critical data is being sent are all encrypted. Secondly, when employees connects remotely via the SonicWALL VPN to access customer's private critical date all traffic is encrypted. Also all wireless traffic is encrypted whenever staff connect wirelessly.

App Assessment

The core application for K124 is Fame. This software has a core data base running on the server in the headquarters. The software is consistently being patched and updated. Fame stores all the students information. This software is protected by all network controls that we have in place.

Multi-factor Authentication

Multi-factor is setup and configured for the Office 365 email accounts. Multi-factor is also setup and configured on the NetExtender private VPN connections from the staff's laptops when they connect remotely back to the main office.

Disposal of Customer Info

This area of risk control is related to the end user hardware and network along with software access.

New Computer Hardware

First of all, the computer that the end users work on is decommissioned and the hard drive is destroyed when they receive a new computer.

Employee Leaves Company

When an employee leaves the company for any reason their user account is locked and or deleted and their VPN account is disabled. They no longer

Anticipation & Evaluation of Network

Related to the anticipation various risks The Webroot antivirus solution on all systems at K124 is preemptively scanning several areas of the operating system and monitoring. Also, we have implemented Webroot DNS which on-the-fly scans each site that is browsed throughout the entire organization.

Network RapidFire tools subscription will provide network scanning on all devices, vulnerability scanning and cyber monitoring which detects changes and anomalous activity before attacks happen. Reporting will be provide on an ongoing basis.

Another area of protection is making sure full data and server backups are taking place. K124 has three forms of backups. Number one would be Windows shadow copy snapshot backups, local full server backups and encrypted online backups. Backups are also tested periodically to ensure integrity.

Along with the process mentioned above we also have a process in place to update the firmware on all network hardware and devices. A number of the devices such as firewall and switches are updated manually but others are automated by using built in tools.

Log of Authorized Users'

A log of all activity related to the LAN and WAN systems at K124 are all tracked and logged via multiple systems such as:

- **Windows Server System Logging**: The server tracks every user and all activity related to the entire domain.
- **SonicWALL firewall**: All traffic related to Intrusion Prevention, all WAN traffic, all ports and protocols are logged in the SonicWALL firewall. Also all VPN connection and remote connection activity is logged.

Monitoring & Testing of Safeguards

A log of all activity related to the LAN and WAN systems at K124 are all tracked and logged via multiple systems such as:

- **Windows Server System Logging**: The server tracks every user and all activity related to the entire domain.
- **SonicWALL firewall**: All traffic related to Intrusion Prevention, all WAN traffic, all ports and protocols are logged in the SonicWALL firewall. Also all VPN connection and remote connection activity is logged.
- **Antivirus Software**: The Webroot antivirus solution on all systems at K124 is preemptively scanning several areas of the operating system along with Webroot DNS which on-the-fly scans each site that is browsed throughout the entire organization. Associated with each scan are logs; Scan log, Execution History, Threat Log, and monitoring all background tasks.
- **Network RapidFire Tools**: K124 has an ongoing subscription through RELITEK to provide ongoing penetration testing. Network RapidFire tools will provide network scanning on all devices, vulnerability scanning and cyber monitoring which detects changes and anomalous activity before attacks happen. Reporting will be provide on an ongoing basis.

Train Staff	RELITEK has deployed Webroot Security Awareness Training for all employees. This training consists of short training videos each week that cover all aspects of cyber security, scams, 2Factor Authentication, all aspects of safe and bogus email usage, safe web browsing, various types of attacks such as phishing and ransomware. Other areas of awareness cover compliance and physical security.
Service Provider Monitoring	K124 and along with the management staff has a long-standing relationship with RELITEK Solutions and has an active relationship that fosters ongoing communication and updates related to all areas of the network to mitigate any types of risks.