Book	Board of Trustees Policy
Section	800 Operations
Title	Cyber Security
Code	850
Status	Active
Adopted	February 6, 2023

Agora Cyber Charter School

Board of Trustees

CYBER-SECURITY POLICY

The Board of Trustees of Agora Cyber Charter School ("Charter School") recognizes the role that technology plays in its daily operations. As such, the security of the Charter School's electronic system against cyber-attacks and the prevention of a possible breach of electronic information is a priority of the Board. Therefore, the Board directs the CEO or designee to manage cyber security measures to minimize threats that could lead to significant downtime of the Charter School's systems and to prevent risk to critical systems and member data.

This policy is established to help prevent infection of the Charter School computers, networks, and technology systems from malware and other malicious code. This policy is intended to help prevent damage to user applications, data, files, and hardware.

This policy applies to all computers connecting to the Charter School network for communications, file sharing, etc. This includes, but is not limited to, desktop computers, laptop computers, servers, and any mobile devices.

The Charter School shall, to the extent possible, abide by industry best practices and in accordance with the advice of local, state and federal agencies and regulators.

Definitions

Virus: A program that attaches itself to an executable file or vulnerable application and delivers a payload that ranges from annoying to extremely destructive. A file virus executes when an infected file is accessed. A macro virus infects the executable code embedded in programs and applications that allows users to generate macros.

Trojan Horse: Destructive programs, usually viruses or worms, which are hidden in an attractive or innocent looking piece of software, such as a game or graphics program. Victims may receive a Trojan horse program by e-mail or removable media, often from another unknowing victim, or may be urged to

download a file from a web site or download site.

Worm: A program that makes copies of itself elsewhere in a computing system. These copies may be created on the same computer or may be sent over networks to other computers. Some worms are security threats using networks to spread themselves against the wishes of the system owners and disrupting networks by overloading them. A worm is similar to a virus in that it makes copies of itself, but different in that it need not attach to particular files or sectors at all.

Phishing: The fraudulent practice of sending emails or other messages purporting to be from reputable companies in order to induce individuals to reveal personal information, such as passwords and credit card numbers.

Spyware: Programs that install and gather information from a computer without permission and reports the information to the creator of the software or to one or more third parties.

Malware: Short for malicious software, a program or file that is designed to specifically damage or disrupt a system, such as a virus, worm, or a Trojan horse.

Adware: Programs that are downloaded and installed without user's consent or bound with other software to conduct commercial advertisement propaganda through pop-ups or other ways, which often lead to system slowness or exception after installing.

Ransomware: A type of malware that prevents or limits users from accessing their system, either by locking the system's screen or by locking the users' files, unless a ransom is paid.

CYBER-SECURITY PREVENTION MEASURES TO BE INSTITUTED

The Charter School will, to the extent possible, keep all systems and programs up to date and backed up. The Charter School shall continuously monitor all systems and programs for signs of cyber insecurity.

The Charter School will create prudent and acceptable practices regarding anti-virus management and to educate individuals, who utilize the Charter School's system resources, on the responsibilities associated with anti-virus protection including the use of multi-factor identification practices, strong passwords, and backups.

The Charter School shall educate system users about phishing and other potential risks posed by outside actors attempting to access the Charter School's systems and/or data.

All computer devices connected to the network shall have anti-virus software installed and configured so that the virus definition files are current and are routinely and automatically updated. The anti-virus software must be actively running on these devices. The virus protection software must not be disabled or bypassed without IT approval. The settings for the virus protection software must not be altered in a manner that will reduce the effectiveness of the software. The automatic update frequency of the virus protection software must not be altered to reduce the frequency of updates.

All computer devices will also utilize cloud app security measures, which includes the use of multi-factor authentication applications to ensure secure sign-ins for online accounts associated with the programs utilized by the Charter School. All employees are to only use those programs and apps that are approved by the school for the conducting of school business.

All incoming files through email will be scanned for malware and other potential cyber-security risks.

Every virus that is not automatically cleaned by the virus protection software constitutes a security incident and must be reported to the Service Desk.

CYBER-SECURITY BREACH RESPONSE

Upon the discovery of any suspected cyber security incident, the Charter School shall make the appropriate notification(s) to its insurance carrier(s) as required by any applicable insurance policy.

The Charter School shall identify individuals from different areas of the organization to serve on an Incident Response Team. The Charter School shall then appoint an Incident Response Manager to head the Incident Response Team.

In the event of any disclosure of Personally Identifiable Information, the Charter School shall comply with all applicable local, state and federal law and/or regulations in response to the disclosure.