Russell Byers Charter School

Board of Trustees Policy

INTERNET SECURITY/FIREWALL POLICY

With the recent onset of technological advancements, server security has become vulnerable to numerous threats throughout the web environment. Therefore, the Board of Trustees of the Russell Byers Charter School ("Charter School") recognizes that it is of the utmost importance to ensure that Charter School's internet server is secure. With this in mind, the Charter School has developed the following policy to provide direction in implementing internet server and network security measures.

Definitions

Firewall: Any hardware and/or software designed to examine network traffic using policy statements (rulesets) to block unauthorized access while permitting authorized communications to or from a network or electronic equipment.

Firewall Configuration: The system settings affecting the operation of a firewall appliance.

Firewall Ruleset: A set of policy statements or instructions used by a firewall to filter network traffic.

Host: Any computer connected to a network.

Host Firewall: A firewall application that addresses a separate and distinct host. Examples include, but are not limited to: Symantec's Norton Personal Firewall, Zone Labs' ZoneAlarm, native firewall functionality supplied under operating systems, e.g. Mac OS, Linux, Windows.

Least privilege: This principle means that each individual will have access only to systems and information that he or she *needs* access to for a school-related purpose. Primarily, this principle limits the damage that can result from an accident or error.

Legally/Contractually Restricted Information: Information that is required to be protected by applicable law or statute (e.g., FERPA, HIPPA) or which, if disclosed to the public, could expose Charter School to legal or financial

obligations. Examples include, but are not limited to, occurrences of personally-identifiable information, e.g. social security numbers ("SSNs"), personnel records, student records, medical records, names in connection with SSNs, and credit card numbers.

Network Device: Any physical equipment attached to the Charter School network designed to view, cause, or facilitate the flow of traffic within a network. Examples include, but are not limited to: routers, switches, hubs, and wireless access points.

Network Firewall: A firewall appliance attached to a network for the purpose of controlling traffic flows to and from single or multiple hosts or subnets.

Public Information: Information that is available to all members of the Charter School community and may be released to the general public. Charter School reserves the right to control the content and format of Public Information. This information is not restricted by charter school, state, federal or international statute or law regarding disclosure or use.

Technology Resources: Technologies, devices and resources used to access, store or communicate information. This definition includes, but is not limited to: computers, information systems, networks, laptops, iPads, modems, printers, scanners, fax machines and transmissions, telephonic equipment, audio-visual equipment, digital cameras, wireless reading devices, i.e. Kindles and Nooks, Internet, electronic mail, electronic communications devices and services, multi-media resources, hardware and software, including Moodle software.

User: Any person who has signed Charter School's Acceptable Use and Internet Safety Policy and is permitted by Charter School to utilize any portion of Charter School's Technology Resources including, but not limited to, students, employees, contractors, consultants, vendors, and agents of Charter School.

Use of Technology

Network accounts will be used only by the authorized User of the account for its authorized purpose. The principle of least privilege applies, so Users should only have the privileges they need to perform their assigned tasks -- and no more. All communications and information accessible via the network should be assumed to be the property of Charter School and shall not be disclosed. Charter School reserves the right to review all communication on Charter School's Technology Resources. Users shall respect the privacy of the other Users on the system.

The Users of Technology Resources at Charter School agree that they have the responsibility to act in an ethical and legal manner in accordance with all Charter

School policies, including, but not limited to, Charter School's Acceptable Use and Internet Safety Policy, CIPA Policy, and FERPA Policy, along with all applicable federal and state laws.

Security/Firewalls

Network servers are extremely important for the existence of Charter School. Servers are essential because they store confidential information, valuable resources, e-mails, and other resources of the Charter School community. Once a server is compromised, it may be very difficult to retrieve important documents and files.

Therefore, all important data must be backed-up and Charter School's network must be protected from infiltration by subscribing to network security. A firewall can act as a powerful weapon to detect hacking attempts and notify Charter School of any impending threat.

A firewall is an appliance (a combination of hardware and software) or an application (software) designed to control the flow of Internet Protocol (IP) traffic to or from a network or electronic equipment. Firewalls are used to examine network traffic and enforce policies based on instructions contained within the Firewall's Ruleset. Firewalls represent one component of a strategy to combat malicious activities and assaults on computing resources and network-accessible information. Other components include, but are not limited to, antivirus software, intrusion detection software, patch management, strong passwords/passphrases, and spyware detection utilities.

Firewalls are typically categorized as either "Network" or "Host." A Network Firewall is most often an appliance attached to a network for the purpose of controlling access to single or multiple hosts, or subnets. A Host Firewall is most often an application that addresses an individual host (e.g., personal computer) separately. Both types of firewalls (Network and Host) can be and often are used jointly.

Requirements:

- A Network Firewall is required in all instances where Legally/Contractually Restricted Information is stored or processed.
- A Host Firewall is required in all instances where Legally/Contractually Restricted Information is stored or processed and the operating environment supports the implementation.
    - Both the Network and Host Firewalls afford protection to the same operating environment, and the redundancy of controls (two separate and distinct firewalls) provides additional security in the event of a compromise or failure.

- All maintenance of Network Firewall Rulesets must be performed by the Director of Technology, unless permitted by a documented agreement between Charter School and the school, vendor, consultant, and/or contractor assuming the Firewall Administrator's responsibilities.

- Where equipment is used to capture, process or store data identified as Legally/Contractually Restricted Information and the equipment is accessible via an Internet connection, a Host Firewall appropriately installed, configured and maintained is required where the operating environment supports that installation. The maintenance of the Host Firewall's Configuration and Ruleset is the responsibility of that system's administrator.

Where equipment is used to capture, process or store data identified as internal or public and the equipment is accessible via an Internet connection, a Host and/or Network Firewall is recommended.

Use of a Host Firewall is recommended for any individual Host with access to the Internet; its maintenance is the responsibility of the individual user or designated support personnel.

Procedures:

1. All Network Firewalls installed and implemented must conform to the current standards as determined by Charter School. Unauthorized or non-standard equipment is subject to immediate removal, confiscation, and/or termination of network connectivity without notice.

2. All Firewall implementations must adopt the position of "least privilege" and deny all inbound traffic by default.

3. Firewalls must be installed within production environments where Legally/Contractually Restricted Information is captured, processed, or stored, to help achieve functional separation between web-servers, application servers, and database servers.

4. Firewalls require periodic review to ensure they afford the required levels of protection.

5. Firewall Rulesets and Configurations must be backed up frequently to alternate storage (not on the same device). Multiple generations must be captured and retained in order to preserve the integrity of the data, should restoration be required. Access to rulesets and configurations and

backup media must be restricted to those responsible for administration and review.

6. Network Firewall administration logs (showing administrative activities) and event logs (showing traffic activity) are to be reviewed by the Chief Executive Officer ("CEO") or his/her designee. Appropriate access to logs and copies is permitted to those responsible for Firewall and/or system maintenance, support and review.

Third Party Access

Third Party Access is defined as granting technology resource data access to an individual who is not an employee of Charter School.

Examples of Third Party Access include, but are not limited to:

1. Software vendor who is providing technical support;
2. Contractor or consultant;
3. Service provider; and
4. An individual providing outsources services to Charter School requiring access to applications or data.

Third Party Access is only to be provided after the Third Party has signed a Non-Disclosure Agreement and Charter School's Acceptable Use and Internet Policy, which must be included in their formal contract with Charter School. Charter School students and staff may never permit another individual to utilize their user name to access Charter School's network.

The CEO or his/her designee may develop additional procedures, as needed, to implement this Policy.

TO THE EXTENT THAT ANYTHING IN THIS POLICY COULD BE CONSTRUED TO CONFLICT WITH THE SCHOOL'S CHARTER OR APPLICABLE STATE AND/OR FEDERAL LAWS, THE APPLICABLE STATE AND/OR FEDERAL LAWS AND/OR CHARTER CONTROL.

ADOPTED this 17th day of Sept., 2020