Early Learning Coalition
of Flagler & Volusia

Policy: Data Security Controls

Policy Number: IT01

Effective Date: March 27, 2018

Editions:

The Early Learning Coalition of Flagler and Volusia Counties, Inc. uses physical and system controls to protect information and systems from security threats. Threats to the organization can include theft; unauthorized access; and use, disclosure, disruption, modification, or destruction of information. The Coalition is responsible to its staff, volunteers, and clients to use reasonable defenses against attempts to gain unauthorized access, such as an attack attempting to exploit a vulnerability. This policy addresses the requirements in many of the critical controls in the organization's operations:

Authentication

Authentication is the verification of the user's identity by a system. This is based on the presentation or delivery of unique credentials to that system. The unique credentials can be in the form of various factors. Authentication contributes to the confidentiality of data and the accountability of actions performed on the system by verifying the unique identity of the system user.

Network Access

The Coalition's allows access by staff, volunteers, and others approved to use the organization's systems and disallows access to all others. Authorized individuals may be employees, vendors, contractors, customers, or visitors. Access is provided only to individuals whose identity is established, with levels limited to the minimum required for organizational purposes.

Logging and Monitoring Reports

The Coalition's logging and monitoring reports contain host and network data gathering for review, analysis, and storage. Host data is gathered and recorded in logs and includes detailing of performance and system events, including behavior that may indicate an intrusion. Security logs are retained, allowing the organization to identify security issues and enforce accountability. Security event logs may include operating system access, privileged access, creation of privileged accounts, configuration changes, and application access attempts (both successful and unsuccessful). Confidential applications may require their own logging of significant events.

Intrusion Detection/Prevention

The Coalition may implement a Network Intrusion Detection and Prevention System, if feasible. These systems perform as an access control mechanism, allowing for access based on an analysis of packet headers and packet contents. The functions of the Network Intrusion Detection and Prevention System:

- Monitor and analyze user and system activity
- Audit system configurations and vulnerabilities

- Assess integrity of critical system and data files
- Provide statistical analysis of activity patterns based on the matching to known attacks
- Analyze abnormal activity
- Audit operating system
- Identify potential threats and respond to them swiftly

System Quarantine

Quarantining a system or device is a measure that protects the network from potentially malicious code or actions. If a system or device connecting to a security domain does not meet approved standards, it is placed in a restricted part of the network until it does meet those standards or is permanently removed from the network.

Patch Management

Patches are updates to commercially developed software to correct identified flaws that otherwise can create security or performance vulnerabilities on servers, desktops, laptops, or other organization information device. Effective patch management assists the organization in mitigating the risks associated with software vulnerabilities and ensures that the security and availability of computer systems is not compromised.

Firewalls

Firewalls are employed by the Coalition to protect the network from unauthorized access. Dedicated firewalls must be used on all Internet connections where inbound access is allowed. Firewalls can be separate devices, a component on a larger device, such as a router, or software-based. Firewalls protect systems that contain confidential data within the internal network.

The Organization implements and maintains appropriate firewalls by:

- Defining the type of allowed or disallowed traffic coming into and going out of The Coalition's network. This will be based on the assumption that all traffic not expressly allowed is denied.
- Managing and updating the Organization's firewall, which may include collaboration with a third-party service provider.
- Detailing which protocols and applications can traverse the firewall and under what exact circumstances this can occur.
- Detailing the firewall and security architecture.
- Listing the type of firewall(s) deployed.
- Monitoring firewall traffic.
- Coordinating with security monitoring and incident response procedures.
- Ensuring that a regular external audit is performed of a firewall's configuration and testing of the firewall's effectiveness is performed.

- All activity that passes through the firewall of the Organization must be logged to management stations for routine or periodic log file analysis.
- To ensure maximum security for the Organization network, the firewall itself will be located in a room that is protected by a locked door or within a room where access is restricted to Information Technology staff only.
- The firewall should be protected from external electrical surges via a surge protector designed to protect an Ethernet cable segment. The firewall will be plugged into an uninterruptible power source (UPS).
- Firewall rules must be periodically reviewed to ensure that adherence to current standards and determination if any existing rules may cause security vulnerabilities that were not present when the firewall was last updated.

<u>Virtual Private Network (VPN) and Encryption</u>

All VPN tunnels within the Organization network meet these minimum standards:

- 3DES or stronger tunnel encryption must be used.
- All tunnel keys must be set to expire at least every 24 hours.
- SHA-1 or stronger authentication types must be used.
- Any Symmetric Encryption Keys must be a minimum of ten characters long.
- Any Symmetric Encryption Keys must not be stored anywhere in written or electronic form.

<u>Virus Protection</u>

All Coalition employees must protect against the threat of viruses. When an infected file is opened from a computer connected to the organization’s network, the virus can spread throughout the network and may do considerable damage. The organization examines corporate assets for viruses using multiple methods.

<u>Operating System</u>

The Organization maintains controls to protect operating systems and system utilities. Access to operating systems and system utilities is limited to appropriate technology staff and selected third-party service providers. Access control security software is used to restrict access to operating systems and applications.

System hardening and locking down unnecessary processes improves the Coalition’s information security and further restricts potential unauthorized access to information. Unnecessary processes are stopped and all agency infrastructure devices, including servers, firewalls, router switches, and other components will be hardened and locked down.

Portable Devices

Portable devices, including laptops, smart phones, iPads, netbooks, tablet PCs, personal digital assistants (PDAs), smartphones, and other storage devices, are vulnerable to both physical damage and theft. Both the value of the portable media and the organization information on the media is protected. Employees granted the use of organization-owned equipment protect such equipment and ensure the security of confidential information. All new software and applications are assessed by the Information Technology Department for any potential security impact to the organization. Storage of confidential organization files or information on a mobile device is not permitted without specific approval.

Software Licensing

The Coalition ensures that all software is appropriately licensed and will keep current records of all software licenses. The Information Technology Systems Technician is responsible for periodically reviewing the software inventory to ensure compliance with software license agreements.

Employees are required to comply with all software licenses. Duplication of licensed software must only be performed in accordance with the license agreement.