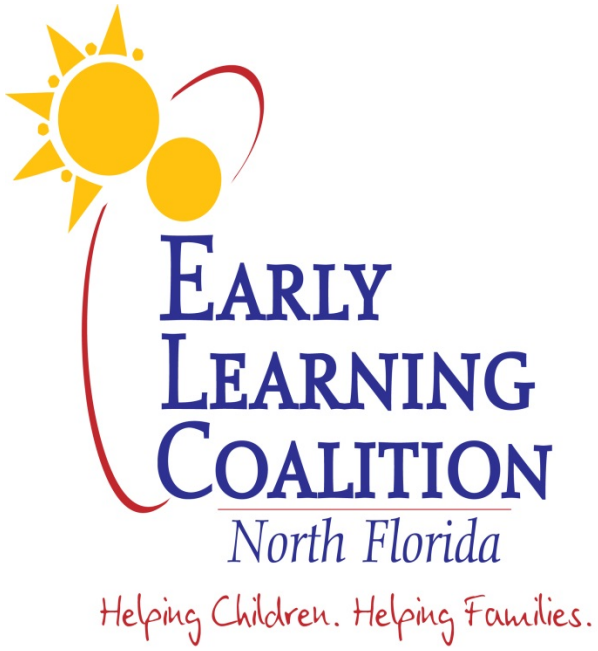

Early Learning Coalition of North Florida, Inc.

Information Technology Systems and Security Policies and Procedures

TABLE OF CONTENTS

IT Systems and Security Policies and Procedures
Receipt and Acknowledgement Form

The Early Learning Coalition of North Florida Information Technology Systems and Security Policies and Procedures describes important information about the Coalition's operations and standards regarding the information technology system, and I understand that I should consult my immediate supervisor regarding any questions not answered in the policy.

Since the information, policies, and procedures described here are necessarily subject to change, I acknowledge that revisions to the manual may occur. All such changes will be communicated through official notices (Board meeting packets and email notifications of updated policies posted to the company share drive), and I understand that revised information may supersede, modify, or eliminate previous policies. For the most current version of this policy, I understand that I am to refer to the folder "Policies and Procedures" on the ELC share drive, where ALL current policies are stored and made available to ALL employees.

I have received the IT policies and procedures, and I understand that it is my responsibility to read and comply with the policies contained within it and any revisions made to it. I acknowledge that if I have any question concerning the terms or operation of any of the policies, that it is my responsibility to obtain clarification from my immediate supervisor and/or the C.E.O.

EMPLOYEE'S NAME (printed): _____

EMPLOYEE'S SIGNATURE: _____

DATE: _____

Chapter 1

GENERAL

IT101 General Scope

Effective Date: 10/01/08
Revision Date: 02/03/10, 04/08/15, 03/16/16, 03/22/17, 06/12/19, 03/11/20

Purpose and Scope

The purpose of this policy is to identify guidelines for the use of the Coalition technologies and communications systems. This policy establishes a minimum standard that must be upheld and enforced by users of the Coalition's technologies and communications systems. Subrecipients of the Coalition must have an equivalent level of security and policy and procedure standard.

Computer and electronic communications resources include, but are not limited to, host computers, file servers, stand alone computers, laptops, PDAs, printers, fax machines, phones, online services, email systems, bulletin board systems, and all software that is owned, licensed or operated by the Coalition.

The policies and guidelines apply to all Coalition systems, whether onsite and connected directly to the Coalition network, or onsite or offsite and connected to the Coalition network by the telephone system or other means. The policies and guidelines cover these systems no matter who is the owner or the method of connection to the network. Employees and registered users are responsible for their own actions, as well as for the actions of any person who they permit to access a Coalition system.

Referenced Legislation and Guidance

For the Coalition's IT policies and procedures, these citations apply and more information can be found in the annual OEL Grant Award Agreement:

- Computer-related Crimes, Chapter 815, F.S
- 2 CFR 200.335, *Methods for collection, transmission and storage of information*
- OEL IT Security Manual (*Program Guidance 300.01)*
- OEL Program Guidance 101.02, *Records Confidentiality*
- OEL IT Security Policy 5.05
- OEL IT Security Policy 5.05.02, *IT Security/Risk Mitigation Services*
- OEL Grant Agreement

(Note: Please find these referenced documents/regulations in the "Referenced Documents-Regulations" folder in the "Policies and Procedures" folder located in the Coalition "Company Share" drive. Contact the Coalition Grants and Operations Manager should there be any difficulty in finding a document or regulation.)

All Coalition IT vendors and Subrecipients/Subcontractors must comply with all security requirements within this policy and as referenced in OEL's IT Security Policy 5.05.02, *IT Security/Risk Mitigation Services.*

Definitions

For purposes of this policy the following definitions shall apply:

Botnets: are networks of computers infected by malware (computer virus, key loggers and other malicious software) and controlled remotely by criminals, usually for financial gain or to launch attacks on websites or networks. If your computer is infected with botnet malware, it communicates and receives

instructions about what it's supposed to do from "command and control" computers located anywhere around the globe. What your computer does depends on what the cybercriminals are trying to accomplish. Many botnets are designed to harvest data, such as passwords, social security numbers, credit card numbers, addresses, telephone numbers, and other personal information. The data is then used for nefarious purposes, such as identity theft, credit card fraud, spamming (sending junk email), website attacks, and malware distribution.

Breach: as defined in Chapter 282.0041, F.S., "Breach" means a confirmed event that compromises the confidentiality, integrity, or availability of information or data.

Breach of Security: as defined in Chapter 501.171, F.S., "Breach of Security" means unauthorized access of data containing personal information. Good faith access of personal information by an employee or agent of the ELC does not constitute a breach of security, provided that the information is not used for a purpose unrelated to the agreement or subject to further unauthorized use.

Confidential (Records): refers to entire record systems, specific records or individually identifiable data that by law are not subject to public disclosure under Article I, Section 24 of the Florida Constitution and Chapter 119, Florida Statutes (F.S.) When applicable, confidentiality covers all documents, papers, computer files, letters and all other notations of records or data that are designed by law as confidential. Further, the term confidential also covers the verbal conveyance of data or information that is confidential. These confidential records may include but not be limited to, social security numbers, parent and child information, payments, childcare providers, household demographics and resource and referrals, which are private and confidential and may not be disclosed to others.

Electronic Communications: shall mean and include the use of information systems in the communicating or posting of information or material by way of electronic mail, bulletin boards, World Wide Web (internet), or other such electronic tools.

Electronic Mail ("email"): an office communications tool whereby electronic messages are prepared, sent and retrieved on personal computers.

Encryption: the process of transforming information (referred to as plaintext) using an algorithm (called cipher) to make it unreadable to anyone except those possessing special knowledge, usually referred to as a key.

Firewall: a device or set of devices configured to permit, deny, encrypt, decrypt, or proxy all (in and out) computer traffic between different security domains based upon a set of rules and other criteria.

Firmware: the combination of a hardware device and computer instructions and data that reside as read-only software on that device.

Hot Fixes: a single, cumulative package that includes one or more files that are used to address a problem in a product and are cumulative at the binary and file level. A hot fix addresses a specific customer situation and may not be distributed outside the customer's organization.

Information Systems: shall mean and include software, electronic communications, computers, networks, servers and other similar devices that are administered by the Coalition and for which the Coalition is responsible.

Internet: a global system interconnecting computers and computer networks. The computers and networks are owned separately by a host of organizations, government agencies, and companies. The internet is the present "information super highway."

Malware: software designed to infiltrate or damage a computer system without the owner's informed consent.

Networks: shall mean and include video, voice and data networks, routers and storage devices.

Online Service (i.e., the Internet, World Wide Web, AOL, etc): is defined as a communications tool whereby business information, reference material and messages are sent and retrieved electronically on personal computers.

PC's: an abbreviation for "personal computers."

Password: a string of characters which serves as authentication of a person's identity, which may be used to grant or deny access to private or shared data.

Personally Identifiable Information (PII): PII means information that can be used to distinguish or trace an individual's identity, either alone or when combined with other personal or identifying information that is linked or linkable to a specific individual. Some information that is considered to be PII is available in public sources such as telephone books, websites, and university listings. This type of information is considered Public PII and includes for example, first and last name, address, work telephone number, and general educational credentials.

Phishing: a form of social engineering where the attacker attempts to trick people into revealing private information by sending spoofed emails that appear to be from reputable companies. Phishing emails provide a link to a seemingly authentic page where you can login and reveal your username, password and other personal identifying information. Online scammers can then use this information to access your accounts, gather additional private information about you, and make purchases or apply for credit in your name. A favorite phishing tactic among cybercriminals is to spoof the display name of an email. If a fraudster wanted to spoof a name of someone in your company, they would create a fake email domain "my-company.com" and then use someone from the company name in the name field.

Protected Personally Identifiable Information (Protected PII or PPII): Protected PII means an individual's first name or first initial and last name in combination with any one or more of types of information, including, but not limited to, social security number, passport number, credit card numbers, clearances, bank numbers, biometrics, date and place of birth, mother's maiden name, criminal, medical, financial records, and education transcripts. This definition does not include PII that is required by law to be disclosed. [2 CFR Part 200.82]

Server: a computer program that provides services to other computer programs in the same or another computer. A computer running a server program is frequently referred to as a server, though it may also be running other client (and server) programs.

Security Incident: as defined in Chapter 282.0041 F.S., "Security Incident" means a violation or imminent threat of violation, whether such violation is accidental or deliberate, of information technology security policies, acceptable use policies, or standard security practices. An imminent threat of violation refers to a situation in which the state agency has a factual basis for believing that a specific incident is about to occur.

Smishing: a combination of the terms "SMS" and "phishing". It is similar to phishing, but refers to fraudulent messages sent over SMS (text messaging) rather than email. The goal of smishing is to capture personal or business information. In order to do this, "smishers" send out mass text messages designed to capture the recipients' attention, while others may provide a fake incentive. If you click on a link in the text message, you will be directed to a fraudulent website that will ask you to enter your personal or business information.

Spam: abuse of electronic messaging systems (including most broadcast media and digital delivery systems) to send unsolicited bulk messages indiscriminately.

Spyware: a type of malware that is installed on computers and collects information about users without their knowledge.

User: refers to employees (whether full-time, part-time or limited term), independent contractors, consultants, and any other user having authorized access to, and using any of, the Coalition's computers or electronic communications resources.

Vendor: someone who exchanges goods or services for money.

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 Microsoft Office programs that allows a user to generate macros.

Vishing: Vishing (voice or VoIP phishing) is an electronic fraud tactic in which individuals are tricked into revealing critical financial or personal information to unauthorized entities. Vishing works like phishing but does not always occur over the Internet and is carried out using voice technology. A vishing attack can be conducted by voice email, VoIP (voice over IP), or landline or cellular telephone.

Website: a location on the World Wide Web, accessed by typing its address (URL) into a web browser. A website always includes a home page and may contain additional documents or pages.

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. The first use of the term described a program that copied itself benignly around a network, using otherwise-unused resources on networked machines to perform distributed computation. 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.

Chapter 2

COALITION IT PROPERTY

IT201 Use of Coalition IT Property

Effective Date: 10/01/08
Revision Date: 08/24/12, 12/04/13, 04/08/15, 03/16/16, 03/22/17, 03/11/20

Acceptable Use of Coalition Property

Use of the Coalition's computers and electronic communications technologies is for program and business activities of the Coalition. These resources shall be used in an honest, ethical, and legal manner that conforms to applicable license agreements, contracts, and policies regarding their intended use.

The Coalition's information systems are to be used predominately for Coalition related business. However, limited personal use may be permitted so long as it conforms to this policy and does not interfere with business operations or an employee's performance of duties.

UNDER ALL CIRCUMSTANCES, PERSONAL USE BY EMPLOYEES MUST COMPLY WITH THE GUIDELINES PROVIDED IN THIS POLICY AND SHALL NOT CONFLICT WITH AN EMPLOYEE'S PERFORMANCE OF DUTIES AND RESPONSIBILITIES FOR THE COALITION. Personal use may be denied when such use requires an inordinate amount of information systems resources (e.g. storage capacity, bandwidth, etc.). All internet software downloads must be granted permission by the Office Manager.

Although incidental and occasional personal use of the Coalition's communications systems are permitted, users automatically waive any rights to privacy.

Waiver Of Privacy

The Coalition has the right, but not the duty, to monitor any and all aspects of its information system, including, but not limited to, monitoring employees use of the internet, reviewing material downloaded or uploaded by employees, and reviewing emails sent and received by employees. Employees waive any right to privacy in anything they create, store, send, or receive on the Coalition's information systems.

In addition, the information, ideas, concepts and knowledge described, documented or contained in the Coalition's electronic systems are the intellectual property of the Coalition. The copying or use of the Coalition's intellectual property for personal use or benefit during or after employment (or period of contract) with the Coalition is prohibited unless approved in advance by the C.E.O.

All hardware (laptops, computers, monitors, mice, keyboards, PDAs, printers, telephones, fax machines, etc.) issued by the Coalition is the property of the Coalition and should be treated as such. Users may not physically alter or attempt repairs on any hardware at any time. Users must report any problems with hardware to the Office Manager.

Use of Computer Workstations and Software

Computer workstations (PCs) are the property of the Coalition and not the personal property of the individual employee. The following shall apply to PC and software use:

Virus Scanners

The Coalition complies with requirements for antivirus programs described in OEL's IT Security Policy. The Coalition maintains current antivirus controls on its computer systems. This includes servers, laptops, and desktop computers. The system will automatically download and distribute virus signature updates to the server, desktop computers, and laptops. The antivirus software is monitored by the Office Manager and the Coalition's IT vendor. File system scans of all systems are conducted automatically. The Coalition's antivirus software protects data, scanned documents, emails and attachments, and internet sites before use. In addition, the Coalition utilizes antivirus programs that scan portable media devices such as flash drives, CD's, and other storage devices before use. Documentation is maintained to verify the purchase and installation of antivirus software by either the Coalition Office Manager or the Coalition IT Vendor.

Any computer used for remote access to the Coalition's and/or OEL's network/databases must have an ICSA (International Computer Security Association) approved antivirus software loaded and updated on a regular basis. This includes any laptop or workstation used by an employee working from home. Employees are prohibited from accessing these networks or databases from home if their personal computing devices do not meet these antivirus software requirements.

Users are prohibited from unloading, disabling, or altering the configuration of the antivirus software. Users are not allowed to bypass the virus scanners when logging onto a PC.

Users are also required to report any suspicious activity on their computers to the Office Manager. This activity includes, but is not limited to: cursor or mouse moving on its own, uncharacteristically slow performance, or a change in behavior of the system, etc. If a virus is found, the user should immediately call the IT support staff so they can inform the user of what steps to follow. If the user should have to leave a message on voice mail, turn the computer off and wait for their response. Do not continue to use the PC if a virus has been found.

Download/Installation of Software

The installation of new software without the prior approval of Office Manager is prohibited. If an employee desires to install any new programs, permission should first be obtained from the Office Manager. Software should not be downloaded from the internet, and employees should never download files from an unknown or suspicious source. This is a common mechanism for the introduction of computer viruses. If internet-based software is needed, the Office Manager should be contacted to perform the download.

Unauthorized Software

No software other than authorized software is to be loaded onto the PC. The Coalition does not condone the illegal duplication of software. The law protects the exclusive rights of the copyright holder and does not give users the right to copy software unless the manufacturer does not provide a backup copy. Unauthorized duplication of software is a federal crime.

Copyrights and License Agreements

It is the Coalition's policy to comply with all laws regarding intellectual property. The Coalition and its employees are legally bound to comply with the Federal Copyright Act (Title 17 of the U. S. Code) and all proprietary software license agreements. Noncompliance can expose the Coalition and the responsible employee(s) to civil and/or criminal penalties. This policy applies to all software that is owned by the Coalition or licensed to the Coalition.

Coalition Ownership – Other IT Categories

The Early Learning Coalition will own and/or have rights to the following types of information technology that was initiated for the sole use and discretion of the Coalition. These types of IT items may include, but are not limited to:

- Cell phone numbers
- Web addresses
- Twitter handles
- Face Book pages
- Blogs
- Other social media
- Includes login ID and passwords (as well as security challenge questions and answers)
- Cloud storage locations (server, drop box, google docs, etc.)
- Equipment issued
- External, offline storage devices

Once a Coalition employee, acting on behalf of the Coalition has initiated/registered/acquired/purchased any of the above items, it becomes the legal property of the Coalition.

Removal of Data Prior to Equipment Disposal

The Coalition (or its IT vendor) will ensure that removal of data, especially sensitive client or operational data, is removed prior to disposing of all technological devices. This includes such items as servers, computer hard drives, laptops, digital copiers, and flash drives. The Coalition will utilize a vendor who will run "file-shredding" software on all electronic media, including computer hard drives, prior to disposing of computer equipment. This software should perform low-level formatting or use a "wipe" utility. The software must overwrite all areas of the computer's hard drive in a manner that makes it impossible for subsequent users to retrieve any of the data on the hard drive. When this is done, the vendor will provide documentation of the actual cleansing activity (and that it has been completed before disposal) with the next monthly billing invoice.

In addition, a safe guard has been added to the inventory report. A column was added to document the date and person responsible for ensuring equipment/devices were properly 'cleansed' of all entity data by the IT Vendor and/or Coalition personnel.

Chapter 3

SECURITY AND MANAGEMENT

IT301 IT Vendor Management/System Performance Monitoring

Effective Date: 10/01/08
Revision Date: 02/04/09, 02/03/10, 02/01/12, 04/03/13, 12/04/13, 04/08/15, 03/16/16, 06/12/19, 03/11/20

IT Vendor Responsibilities

As the Coalition outsources IT services, the management of those services are to be regulated and reviewed on a constant basis. The IT vendor is responsible for monitoring adequacy of system hardware, performance and capacity-related issues, routine maintenance of systems, ensuring systems are adequately protected, ensuring systems are updated and backed up daily, making recommendations, and assisting the Coalition when needed. The IT vendor is also responsible for establishing new hire user accounts, resetting user accounts, and deleting user accounts when requested from the Coalition.

At a minimum, the IT vendor must implement and maintain the Coalition's network by monitoring and updating the following items:

1. Upgrade firmware on firewalls
2. Monitor firewall logs
3. Report unauthorized access attempts to proper authorities
4. Maintain network connectivity
5. Apply software patches and security hot fixes to all servers and PC's
6. Test all software/hardware after installation of updates
7. Configure network access for PC's
8. Maintain databases
9. Update antivirus/anti-malware software
10. Monitor antivirus threats
11. Manage spam filtering services
12. Manage secure offsite backup of crucial files and databases
13. Set up network printers/scanners/copiers
14. Troubleshoot computer/network/printer related errors
15. Remove malware from PC's
16. Replace and/or upgrade equipment as needed
17. Move IT related equipment during workspace/office transfers
18. Configure software to interface with industry-specific databases
19. Design and plan upgrades to network and software packages
20. Implement new technologies to better office productivity
21. Provide secure remote access
22. Maintain business continuity/disaster recovery plans and test
23. Perform monthly backup and recovery testing and provide evidence of this with each monthly billing invoice
24. Ensure removal of data, especially sensitive client or operational data, prior to disposing of all technological devices, and provide evidence of this with the next montly billing invoice each time this is done. This includes such items as servers, computer hard drives, laptops, digital copiers, and flash drives.
25. Monitor adequacy of system hardware, performance and capacity-related issues.

IT Vendor Employee Assignment Approval

At the time of the IT vendor contract approval, or change in staff during the course of a contract, the Coalition will supply the Contractor with the "Contract Employee Request and Approval Form" to ensure

all applicable screenings are processed. The IT vendor Contractor will have to submit the completed form with the cleared level II background screening documents, job descriptions, resume/work history, educational credentials and licenses required.

Once the Coalition has reviewed all documents, the Office Manager will approve, sign, date, and send back to the Contractor allowing the staff person to work on the Coalition's contract. If they are not approved, the Coalition's Office Manager will sign THAT portion of the form and follow up with the Contractor regarding that decision.

IT Vendor Capabilities and Performance

When selecting a new IT vendor, or monitoring IT vendor performance, the IT vendor must have the capability to perform remote technical assistance with a response time of no more than four hours, after receiving the request for assistance. The IT vendor must also have the capabililty to password protect and block access as needed.

The IT vendor is required to conduct monthly monitoring of all Coalition IT systems and make necessary updates, install applicable releases, and make needed changes to the system. Annually the IT vendor performs a needs assessment and policy review, then makes recommendations to the Coalition.

Upon annual contract renewal, the Coalition reviews its satisfaction with the vendor's perfomance and activities as it pertains to the vendor's service level agreement.

IT302 User Management

Effective Date: 10/01/08
Revision Date: 02/04/09, 04/08/15, 03/11/20

New Coalition Employees

Upon hire, all Coalition employees are given the Coalition's current IT policy for receipt and review. The employee documents understanding of the policy and their responsibility to secure Coalition IT assets by signing an IT Systems and Security Policies and Procedures Receipt and Acknowledgement Form. In addition, those employees who, as part of their job duties, will have access to the Single Statewide Information System (SSIS) will review and sign the "OEL's Memorandum of Understanding and Data Security Agreement" (data access and security form) prior to obtaining access and training, and annually thereafter. For auditing purposes, the Coalition maintains documentation of the actual antivirus/data security training materials and staff completion of the trainings.

Florida Computer Crimes Act

As the Coalition, through multiple funding sources, has access to sensitive computerized data, all employees are required to understand and comply with the Florida Computer Crimes Act, Chapter 815, Florida Statutes. The minimum security requirements are: passwords are not to be disclosed and information is not to be obtained for the individual or another person's personal use. Security violations may result in disciplinary action.

Confidentiality

All information about individuals, clients or community members served by the Coalition is confidential. No information may be shared with any person outside the Coalition without the prior written approval of the individual, family, or the Coalition. See Coalition Confidentiality Policy **#OP201**.

IT303 Access and Security

Effective Date: 10/01/08
Revision Date: 02/04/09, 02/03/10, 02/02/11, 02/01/12, 08/24/12, 03/16/16, 03/22/17, 06/12/19

Referenced Legislation and Guidance

OEL Grant award Exhibit I, Section F, *Breach of Security/Confidentiality*

(Note: Please find these referenced documents/regulations in the "Referenced Documents-Regulations" folder in the "Policies and Procedures" folder located in the Coalition "Company Share" drive. Contact the Coalition Grants and Operations Manager should there be any difficulty in finding a document or regulation.)

Access Controls

The confidentiality and integrity of data stored on agency computer systems must be protected by access controls (both on-site and remotely) to ensure that only authorized employees have access. The Coalition maintains compliance with all OEL IT Security policies and procedures. Access shall be restricted to only those capabilities that are appropriate to each employee's job duties. All staff (and subrecipient/ subcontractor staff) with access to ELC data systems complete "OEL's Memorandum of Understanding and Data Security Agreement" upon hire and/or position (responsibility) transfer and annually thereafter.

Employees assume all responsibility for their access to the Coalition's information systems. Passwords or access codes must not be shared with others. Any individual password to access the information systems belongs to the Coalition and information regarding usage of the Coalition's information systems is accessible at all times by management for any business purpose. Unauthorized access to information systems is prohibited. No one should use the ID or password of another; nor should anyone provide his or her ID or password to another, except in cases necessary to facilitate computer maintenance and repairs and then only to authorized Coalition Information Technology staff, management, or contracted vendor of IT services. When any user terminates his or her relationship with the Coalition, passwords are changed immediately and his or her access and use of the Coalition's information systems is prohibited.

Physical Security and Access

The Coalition's server is provided by the Coalition's IT vendor and is housed in a secured datacenter. The datacenter has an emergency lighting device within reach, or an emergency lighting system. In addition, the datacenter has a gas based fire extinguishing system. The Coalition, through its IT vendor, uses a cloud-based server.

All critical computer equipment is stored in secure locations and access is restricted to only those individuals who require such access for the performance of their job responsibilities.

Access to network and Windows servers is privileged to the Coalition's IT staff and/or IT vendor who require this level of access based on their function and training levels.

The Coalition's staff have controls and processes in place to physically safeguard the entity's operating systems. The Coalition currently complies with requirements described in OEL IT Security Policy 5.05.02.17, *Physical and Environmental Security*.

A list of such controls for computer equipment include, but are not limited to:

- Heating/cooling standards
- Smoke detectors

- Fire suppression
- Uninterruptible power supplies
- Locks/access
- Alarms
- Cameras
- Instructions for visitors

Password Security

No passwords will be allowed that block entry to a PC or to specific applications or files without prior approval from the employee's supervisor. Users are responsible for safeguarding their login passwords. Passwords may not be shared, printed, or stored online. Users should not leave their computers unattended without logging off. If a user suspects that the secrecy of their password has been compromised they should report this to the Office Manager immediately and initiate a password change request.

For all passwords the Coalition follows the OEL IT Policy 5.05.02.32, which requires ten minimum protocols for creating passwords:

1. Passwords should contain at least eight (8) characters and contain a combination of letters, numbers, and special characters.
2. Passwords cannot be reused for at least six (6) changes.
3. Never assign a login account a password that is the same string as the employee ID or that contains the employee ID (e.g., "bob123" is not an appropriate password for employee "bob").
4. Never set any password equal to the null string (i.e., a blank password), which is equivalent to no password at all.
5. Passwords should not be a dictionary word in any language.
6. Passwords should not contain any proper noun or the name of any person, pet, child, or fictional character.
7. Passwords will not contain any associate serial number, social security number, birth date, telephone number, or any information that could be readily guessed about the creator of the password.
8. Passwords should not contain any simple pattern of letters or numbers, such as "xyz123."
9. Passwords should not share more than three (3) sequential characters in common with a previous password (i.e., do not simply increment the number on the same password, such as fido1, fido2, etc.).
10. Use a password that is easy to remember (e.g., a phrase, line from a song, or nonsense words) and that you can type quickly.

Although OEL policy allows for 90 day use of passwords, and allow to reuse passwords after six changes, the Coalition passwords are changed every 60 days and unique passwords are required at each change. The IT vendor ensures that password updates are set up to be generated on demand every 60 days, and that the new password meets the password criteria.

Other OEL policy protocols for passwords require guidelines for the storage and visibility of passwords and certain instructions on how to setup and assign passwords (for example, avoid using the "remember password" feature on web sites and other applications).

After five attempts to access a system with incorrect passwords, that system will be subjected to a lockout time of 10 minutes. This lock feature is set to mitigate brute-force based attacks.

In addition to password security, all Coalition PC's are protected by installed 10 minute time out screen savers, requiring the user's password to renter their PC's.

Database Security

The Coalition complies with requirements for restrictions on access to sensitive or confidential data described in OEL's IT Policy and Program Guidance 101.02, *Records Confidentiality.* This includes identifying and safeguarding confidential records, Personally Identifiable Information (PII), and Protected Personally Identifiable Information (PPII). *(Please refer to "Definition" section of this policy for more information on these items, as defined by OEL Program Guidance 101.02, Records Confidentiality). (Also refer to the Coalition's Confidentiality policy* ***#OP201****.)*

Database Access is granted to users via the application level only. Changes at the database level are permitted by the database administrator only. Application controls are used to ensure proper access to information within applications based on the responsibility of the staff member. Log files are maintained for changes to all databases.

Mobile Computing Devices are strictly controlled by the Early Learning Coalition. This policy applies to all Coalition-owned mobile devices including, but not limited to laptops, smart phones, tablets and external hard drives/flash drives. Such devices are limited in use and are only serving in the capacity of an access agent to the primary server. In the event of the loss or theft of a laptop, no information would be present on the device. In addition, the Coalition utilizes media storage devices that are password protected and scanned for viruses before each use. The devices (flash drives, thumb drives, laptops, email transmissions, etc.) shall not contain confidential data unless the device is fully encrypted and password protected. In the event of a loss or theft of a smart phone, tablet or other mobile device, the Office Manager will ensure the Coalition's IT Vendor performs a "remote wipe" of the device clearing it of any Coalition information.

Portable Storage Media or Peripheral Device Security
The Coalition, including its employees, subcontractors, agents, or any other individuals to whom the Coalition exposes confidential information obtained under this agreement, shall not store, or allow to be stored, any confidential information on any portable storage media (e.g., laptops, thumb drives, hard drives, etc.) or peripheral device with the capacity to hold information without encryption software installed on the devices meeting the standards prescribed in the National Institute of Standards and Technology Special Publication 800-111 [http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-111.pdf].

Remote Access is provided to all Coalition staff. Encryption is used on both the data sent from and to their workstation. Log records are maintained on all workstations and firewall logs are monitored for unusual activity. The Coalition prohibits the use of personal devices to download or store sensitive or confidential data.

Access to the Coalition's Internal Network is restricted by a hardware firewall. The firewall performs multiple network and security functions such as antivirus, antispyware, firewall, intrusion prevention, and device and application control for complete workstation protection. The network is further protected from spam and viruses by a third party filtering system. In addition, the Coalition is protected against email information loss and business disruption during planned or unplanned outages by access to a web-based email console. During an outage, all inbound and outbound email continues to be filtered to protect the Coalition from threats.

Electronic Imaging and Signatures

Electronic imaging is used to generate official operating records and transaction files. The Coalition has an effective system of controls in place that ensures digital images of the original paper document are accurately represented because staff scan all documents in their entirety.

Staff are instructed to retain all documents per the Coalition's record retention policy to ensure access to the images are not destroyed, but remain accessible until the applicable retention period expires.

If changes to an electronic image are necessary and authorized, staff are instructed to save a copy of the unaltered, original file.

Electronic Signatures must be unique to the signer. To utilize electronically signed documents, the Coalition ensures that signers use a unique signature they control which can be verified via a mechanism such as login or IP address of the signer in a read only format so as not to be altered.

Security and Problem Management

The Coalition's IT vendor records all reports of problems, security incidents, and Coalition requests for services to ensure that these events are responded to and/or resolved within the required four hour response time. In addition, the IT vendor must have the capability to install/perform an automated email alert system, with the firewall, to report any unauthorized or malicious activity.

The Coalition is also required to document and provide the following details for any/each incident, and report to OEL:

(i) The nature of the unauthorized use or disclosure
(ii) The confidential information used or disclosed
(iii) Who made the unauthorized use or received the unauthorized disclosure
(iv) What the Coalition has done or shall do to mitigate any harmful impact of the unauthorized use or disclosure and
(v) What corrective action the Coalition has taken or shall take to prevent similar future unauthorized use or disclosure incidents.

Breach of Security or Security Incident

Coalition staff are required to report any breach/security incidents. The Coalition is also required to report to OEL in writing within 24 hours after the Coalition learns of the security incident or breach. (For more information see OEL Grant award Exhibit I, Section F, *Breach of Security/Confidentiality.)*

IT304 Change Management

Effective Date: 10/01/08
Revision Date: 02/04/09, 03/16/16, 03/11/20

Coalition Employee Changes

When a Coalition employee is hired, terminated, or changes job descriptions/roles, the access settings to the Coalition's IT system must be modified. The procedure for these changes are as follows:

1. The Coalition Office Manager initiates the change request (new account, modified access, or terminated account), by email to the IT vendor.
2. The IT vendor makes the modification on the Coalition IT system.
3. The IT vendor then emails the Office Manager verification of request completion. The verification email is then filed with the Office Manager's IT files, secured in a filing cabinet.

Periodic user system access level review is performed by the C.E.O., or designee, with the assistance of the IT vendor. In addition, the IT vendor performs access reviews monthly, either onsite or remotely. Any needed changes such as access levels or access blockage ar e made immediately.

The Coalition's IT Vendor has procedures in place to address and document the tasks that activate access to Coalition systems for incoming staff and to deactivate/remove access to Coalition systems for outgoing employees. These include:

- Documentation for managing access criteria for information resources.
- Audit trails to provide accountability for all accesses to confidential and exempt information and software.
- Audit trails for all changes to automated security or access. Examples include removal of access privileges, computer accounts and authentication tokens.

Termination of Coalition Employment

Should a Coalition employee resign or be terminated, all files on the PC become the property of the Coalition. Copying of such files for personal use is prohibited. In addition, the employee's user accounts are removed or inactivated from Single Statewide Information System (SSIS), and/or the Coalition network immediately.

Procedures for unfriendly termination(s) include prompt removal of system access initiated by the Coalition's Office Manager (or C.E.O.), and completed by the Coalition's IT Vendor.

Part of the Coalition's Office Manger's employee termination tasks is the processing of any (and all) returned office information resources (property, data, etc.).

Chapter 4

BACKUP SYSTEMS

IT401 Backup Systems and Storage

Effective Date: 10/01/08
Revision Date: 02/03/10, 04/08/15, 03/16/16, 06/12/19

Battery Backup

The Coalition utilizes emergency battery backup devices to ensure productivity during times of possible electronic interference.

Offsite Backup and Storage

The Coalition maintains backup copies of the records through the use of a network server data backup service, provided by the IT vendor, from an offsite location. The backup files must be encrypted and the offsite storage must have a security level of at least a "Tier 4" secure data location. The vendor is required to sign the Coalition's confidentiality agreement (policy **#OP201**) before services are provided, and the backups are performed daily. Access to backup files shall be limited to those employees that it is appropriate. Multiple copies of backup files are recommended as to not overwrite the most recent backup. For auditing purposes, the IT vendor will provide evidence of the backup activities with each monthly billing invoice.

Data Backup and Restore Testing

The Coalition's IT vendor is required to perform regularly scheduled tests of its capability to restore data files from backup storage. At a minimum, these tests must be done monthly. In addition, the IT vendor will provide evidence of the recovery testing with additional documentation submitted with each monthly invoice.

The Coalition complies with requirements for data backups described in the OEL IT Policy.

The IT Vendor is responsible for ensuring procedures are in place to perform:

- nightly backups
- annual review and recommendations for updates to policies and processes for changes in IT operations
- review of the backups
- testing and restoring of backup files, as identified as important by the Coalition

The Coalition is responsible for ensuring that the above services are completed and documented.

Chapter 5

REVIEWS

IT501 Systems and Policies Review

Effective Date: 10/01/08
Revision Date: 02/04/09, 06/26/14, 03/11/20

Annual Review

Annually the Coalition's C.E.O. reviews the IT vendor's needs assessment and recommendations, has the IT vendor and staff review the IT policy, and approves necessary updates to both the IT system and IT policies and procedures.

As the Coalition's Board approves any policy changes, all employees are provided the most current version on the ELC share drive. Once the revisions are processed, the Grants and Operations Manager sends an email alert to all employees that the updated policies are available on the ELC share drive. Employees are aware of this process, as outlined in the IT Systems and Security Policies and Procedures Receipt and Acknowledgement Form.

System Updates and Maintenance

The Coalition performs system updates and maintenance through the Coalition's IT vendor. Scheduled updates and maintenance are performed monthly, and on an "as needed" basis.

All update and maintenance records are kept by the IT vendor and are available upon request.

Chapter 6

Online Services and Emails

IT601 Use of Online Services and Emails

Effective Date: 10/01/08
Revision Date: 02/04/09, 02/02/11, 08/24/12, 03/22/17, 01/24/18, 06/12/19, 03/11/20

Use of Online Services (Internet, World Wide Web, AOL, etc)

Online Services' sites can and do monitor access and usage and can in some cases, identify individuals accessing their services. Thus, Coalition employees should be mindful that accessing a particular bulletin board or website leaves company identifiable electronic "tracks", even if the employee merely reviews or downloads the material and does not post any message.

Employees should also be aware that the Coalition reserves the right to routinely monitor without prior notice, online services access and usage to ensure that the system is being used for Coalition purposes according to this policy and to ensure that the Coalition's policies prohibiting harassment and inappropriate behavior are being followed. Therefore, employees should access sites that are necessary for Coalition business. Inappropriate use may subject an employee to disciplinary action up to and including termination of employment.

Use of Electronic Mail and Online Services

The email and internet system is intended to be used to promote the effective performance of the Coalition's business. While it may be acceptable to send or receive personal messages of a limited number and frequency, personal use of the email system must be kept within the bounds of efficiency and good judgment and under no circumstances should interfere with an employee's performance of job duties or violate Coalition policies regarding appropriate workplace behavior.

Employees should exercise care in the use of email and in the handling of email attachments, and be aware of phishing emails and smishing and vishing practices. (See explanations to these terms in policy **#IT101**, definitions section.) If an email is from someone you do not know, or if you were not expecting an attachment, do not open it and do not forward it. Delete it. These type emails are known as spam, chain, or other junk email. The user should contact the Office Manager for assistance if there are questions as to the validity of the message and attachment.

Confidentiality

All newly hired employees must read the Coalition's Confidentiality policy **(#OP201**) and procedures and sign the Coalition's Employee Confidentiality Agreement form during orientation. All email/internet records are considered Coalition records and should be transmitted only to individuals who have a business need to receive them. This applies to both company proprietary information or confidential material protected by the attorney-client privilege.

In some cases, sensitive information should not be sent via email such as social security numbers, non-abbreviated names of clients and/or children, information that could be considered personal in nature (such as medical or financial information), etc. This type of information should be transmitted through a more secure source, such as the OEL "VPN Portal SharePoint" website, or other forms of secured communication.

Public Disclosure

Additionally (as Coalition records) email/internet records are subject to disclosure to law enforcement or government officials or to other third parties through subpoena or other process. Consequently, employees should always ensure that the business information contained in email or internet messages is accurate, appropriate and lawful. Email/internet messages by employees may not necessarily reflect the view of the Coalition, its officers, directors or management. Abuse of the email/internet systems through

unacceptable personal use, or use in violation of law or Coalition policies, may result in disciplinary action up to and including termination of employment.

The Coalition reserves the right to disclose employee email messages or internet records to law enforcement or government officials or to other third parties, without notification to or permission from the employees sending or receiving the messages. As a condition of initial and continued employment, all employees consent to Coalition review and disclosure of email messages and internet records. In addition, email messages for which the computer system has a record will be stored and retained in accordance with the Coalition's records management/retention policy **#F705**. Full system backup images are retained by the Coalition for a period of seven days; however, there is not an automated archive solution for files or emails, and it is up to the Coalition staff to preserve records according to the Coalition's retention policy and state public records/record retention requirements. All staff should remember –

- The definition of public records includes any/all documents in any/all formats when such communications are made in connection with or relate to the Coalition's business operations.
    - Includes communications (such as texts, emails and voice messages) made on personal cell phones, smart phones, tablets and other mobile devices
    - Includes Facebook or other social media transmissions

Coalition files/records/data items should not be deleted by staff unless/until the record retention period for such files has expired. For more detailed instructions (on what data files can be deleted and when), please contact the Coalition's Records Custodian.

Appropriate Use

Employees should be mindful that when they browse the internet, post information on websites, or send email containing the Coalition's domain address, they are representing the Coalition—not merely themselves—in a public medium. Under no circumstances should an employee's use of the internet compromise the legitimate business interests of the Coalition or give rise to illegality.

Foul, offensive, defamatory, pornographic or other inappropriate communication is strictly prohibited. Further, the Coalition prohibits website posting or email messages containing offensive material, remarks based on sex, race, ethnicity, national origin, disability, marital status, age, off-color remarks or jokes, or disparaging statements about any employee, supervisor, board member, community partner, or person associated with the Coalition in any way. Employees may not use the internet to access, view or download inappropriate materials, including but not limited to harassing or offensive materials, or materials that disparage or demean persons on the above described bases. Employees who send out abrasive, harassing, or discriminatory email messages or who visit inappropriate sites are subject to disciplinary action up to and including termination of employment.

IT602 Cyber Communication and Social Media Use by Employees

Effective Date: 04/08/15
Revision Date:

Overview

The same principles and guidelines that apply to your activities as an employee in general, as found throughout this manual and in your job description, apply to your activities online. This includes forms of online publishing and discussion, including blogs, wikis, file sharing, user-generated video and audio, virtual worlds and social networks.

The Coalition trusts and expects employees to exercise personal responsibility whenever they participate in social media. This includes not violating the trust of those with who we are engaging.

The Coalition expects all employees utilizing social media will recognize and follow the guidelines included within this policy. Failure to do so could result in disciplinary action, up to and including termination.

Policy Expectations

- Always consider the power of your comments and contemplate the impact of your post on your reputation and that of the Coalition before you publish it.
- Respect all confidential and proprietary information that you possess as a result of your relationship/employment with the Coalition. Secure written permission to publish or report on conversations that are meant to be private or internal to the Coalition. Examples of confidential information include, but are not limited to participant information*, confidential academic information*, proprietary data, internal policies and memorandums, and all proposed and executed organizational strategies.
  Note: *Please refer to the Coalition's confidentiality policy **#OP201** for further instructions regarding publication of participant information and/or photographs and media release forms.
- When disagreeing with others' opinions, be appropriate and professional in doing so when posting such disagreements on social media sites.
- When posting about your work at the Coalition, use your real name, identify that you work for the Coalition and the position you hold. Be aware of your association with the Coalition in online social networks. If you identify yourself as an employee of the Coalition, ensure your profile and related content is consistent with how you wish to present yourself with colleagues and participants.
- Respect your audience: Don't use slurs, personal insults, obscenity, or engage in any conduct that would not be acceptable in the Coalition workplace. You should also show proper consideration for others' privacy, and show proper judgment regarding topics that may be considered objectionable or inflammatory.
- Vulgar, obscene, threatening, intimidating, harassing, or discriminatory behaviors on social media sites may result in an employee's immediate termination.

Chapter 7

MISUSE OF COALITION IT SYSTEMS

IT701 Misuse of Computers and IT Systems

Effective Date: 10/01/08
Revision Date: 01/24/18, 03/11/20

Misuse Use of Computers and Electronic Information Systems

Misuse of Coalition electronic information systems is prohibited. Although most users strive for acceptable and responsible use of the systems and resources, inexperienced users may unwittingly engage in behaviors that violate the principles and guidelines of responsible and acceptable use. To that end, this section outlines some of the more common forms of violations that occur. These examples should not be interpreted as an exhaustive list of violations. Questions regarding the appropriateness of specific behaviors should be directed to the Office Manager.

Misuse or violations include but are not limited to the following:

1. Viewing, listening, or engaging in any communication that is objectionable, discriminatory, defamatory, pornographic, obscene, racist, and sexist or that evidences religious bias, or is otherwise of a derogatory nature toward any specific person, or toward any race, nationality, gender, marital status, sexual orientation, religion, disability, physical characteristic, or age group.

2. Browsing, downloading, forwarding and/or printing pornographic, profane, discriminatory, threatening or otherwise offensive material from any source including, but not limited to, the Internet.

3. Engaging in any communication that is in violation of federal, state or local laws, or using information systems for any illegal or unauthorized purpose.

4. Using electronic communications to harass or threaten other employees in such a way as to create an atmosphere, which unreasonably interferes with their work environment. Similarly, using electronic communications to harass or threaten other information recipients in addition to Coalition users.

5. Promoting religious beliefs or tenets.

6. Campaigning for or against any candidate for political office or any ballot proposal or issue.

7. Sending, forwarding, redistributing or replying to “chain letters” or sending chain letters or unauthorized mass mailings or transmitting a crippling number of files across a network.

8. Using unauthorized passwords to gain access to another user’s information or communications on the Coalition’s systems or elsewhere.

9. Advertising, solicitation or other commercial, nonprogrammatic use.

10. Attempting to modify or remove computer equipment, software, or peripherals without proper authorization.

11. Violating any software license or copyright, including copying or redistributing copyrighted software without the written authorization of the software owner.

12. Knowingly introducing a computer virus into the communications systems or otherwise knowingly causing damage to the systems, such as launching a computer worm, computer virus or other rogue program.

13. Using the systems in a personal manner that interferes with normal business functions in any way, including but not limited to excessive recreational or nonbusiness use, streaming audio from the internet during business hours, stock tickers, internet gaming, installing unauthorized software, etc.

14. Excessive personal use of technologies that preempts any business activity or interferes with the Coalitional productivity.

15. Sending abusive, harassing, obscene, hoax or forged messages, including messages sent under someone else's username.

16. Sending email messages under an assumed name or obscuring the origin of an email message sent or received.

17. Gambling or engaging in any activity or action through the use of electronic information systems that violates Coalition policies and regulations, or federal, state, or local laws.

18. Engaging in any activity that is in violation of the Coalition's Code of Ethics (policy **#OP202**) and/or policies and procedures, including this policy.

Disciplinary Action for Violations

The Coalition requires all users (employees, consultants, and outsourced vendors conducting business on behalf of the Coalition) to adhere to all Coalition Information Technology Systems and Security Policies and Procedures. Violations of this policy will result in disciplinary action up to and including termination of employment or cancellation of contracts.

Reporting of Suspected Violations

Suspected violations of these policies should be immediately and confidentially reported to the C.E.O. If the employee does not prefer to discuss it with the C.E.O., the employee may contact any member of the Executive/Administrative Committee.

The Coalition reserves the right to install programs that monitor employee use of the internet and electronic communications systems, and to act on any violations of these policies found through use of such programs. The Coalition further reserves the right to examine any and all electronic communications sent or received by employees via the Coalition's electronic communications systems.