Governed by: IT Administration
Approval Date: November 1, 2016 **Last Updated:** 5/3/2022
Policy: Acceptable Use of CEO IT Systems

Overview of Purpose:

The purpose of the CEO Acceptable Use Policy is to establish acceptable practices regarding the use of CEO Information Technology Resources in order to protect the confidentiality, integrity and availability of information created, stored or transmitted over those resources. This policy is designed to protect CEO, our employees, customers and other partners from harm caused by the misuse of our IT systems and our data.

This policy establishes expectations regarding use of CEO's Technology Resources. When using these resources, users are expected to adhere to the expectations enumerated herein as well as all other CEO policies. Failure to do so may result in corrective action, up to and including termination.

Should any employee be unclear on the policy or how it impacts their role they should speak to their manageror IT Staff.

Contents:

- Internet Access
- Incidental Personal Use

Scope

This policy applies to all of CEO's Technology Resources including, without limitation, desktop and portable computer systems, fax machines, Internet access, voicemail, electronic mail (e-mail), and its intranet.

This policy applies to Technology Resources that are owned or leased by CEO, that are used on or accessed from CEO premises, or that are used on CEO business. This policy also applies to all activities using any CEO-paid accounts, subscriptions, or other technical services, such as Internet and World Wide Web access, voice mail, and e-mail, whether or not the activities are conducted from CEO premises.

Acceptable Use

CEO's Technology Resources are provided for the benefit of CEO and its customers, vendors, and suppliers.

Misuse of CEO's Technology Resources can include both deliberate and inadvertent actions and the repercussions of misuse can be severe. Potential damage includes, but is not limited to, malware infection (e.g., computer viruses), legal and financial penalties for data leakage, and lost productivity resulting from network downtime.

Everyone who works at CEO is responsible for the security of our IT systems and the data on them. You may use the CEO's Technology Resources for lawful and businesses purposes and in accordance with this policy.

Sending, saving, or viewing offensive material is prohibited. Messages stored and/or transmitted over CEO's Technology Resources must not contain content that may reasonably be considered offensive to any Employee. Offensive material includes, but is not limited to, sexual comments, jokes or images, racial slurs, gender-specific comments, or any comments, jokes or images that would offend someone on the basis of his or her race, color, creed, sex, age, national origin or ancestry, physical or mental disability, veteran status, marital status, as well as any other category protected by applicable law. Any use of CEO's Technology Resources to harass or discriminate is unlawful and strictly prohibited.

Further, any content stored, transmitted, or otherwise viewed or used on CEO Technology Resources must not contain any material that is defamatory, obscene, indecent, abusive, or violent. Content must not violate the legal rights (including the rights of publicity and privacy) of others employees, or be likely to deceive any person, promote any illegal activity, or advocate, promote, or assist any unlawful act.

In addition, the following uses of CEO's Technology Resources is strictly prohibited:

- Using CEO's Technology Resources in any way that violates any applicable federal, state, local, or international law or regulation is strictly prohibited.
- Transmitting, sending or procuring any "junk mail," "chain letter," "spam," or any other similar solicitation.
- Impersonating or attempting to impersonate CEO, another employee, or any other person or entity.

- To engage in any other conduct that may cause financial harm to CEO or exposes it to liability.
- Use CEO Technology Resources in any manner that could disable, overburden, damage, or impair the Resources.
- Use any device, software, or routine that interferes with the proper working of CEO Technology Resources.
- Introduce any viruses, Trojan horses, worms, logic bombs, or other material that is malicious or technologically harmful.
- Attack CEO Technology Resources via a denial-of-service attack or a distributed denial-of-service attack.
- Otherwise attempt to interfere with the proper working of CEO Technology Resources.

Access to Information/Data

All data created or stored on or transmitted through CEO's Technology Resources is the property of CEO. While CEO respects the individual privacy of its employees, that privacy does not extend to an employee's work-related conduct or use of CEO's Technology Resources.

Employees are advised that any and all telephone conversations or transmissions, electronic mail or transmissions, or internet access or usage by an employee by any electronic device or system, including but not limited to the use of a computer, telephone, wire, radio or electromagnetic, photoelectronic or photo-optical systems may be subject to monitoring at any and all times and by any lawful means. As a result, all employee communications and use of the Internet that occurs on CEO's Technology Resources are not considered private. Therefore, employees should treat all activities as such. CEO reserves the right to monitor employee use of its Technology Resources at any time. ***Employee use of these resources constitutes their consent to CEO's accessing, intercepting, monitoring and disclosure of any matter stored in, created, received or sent over those resources.***

Users should be aware that CEO will take all possible measures to minimize the risk of vulnerability and/or breach with regard to the confidentiality of information stored on any CEO system except where required to do so by local laws.

Any information that is particularly sensitive or vulnerable is encrypted and securely stored on CEO server storage so that unauthorized access is prevented.

CEO can access, intercept and monitor use of and data created, stored or transmitted through its ITsystems at any time. This may include, but is not limited to, the examination of the content stored within the email and data files of any user, and examination of the access history of any users.

CEO reserves the right to audit networks and systems to ensure compliance with this policy and for other business purposes.

Access Management:

- Access to information is based on a "need to know" system. IT maintains an agency-wide "User List" with permissions/access based on role. Users should only access the

libraries, files, data, programs, and directories that are related to their work duties.

- Users are permitted to access only those network files on the G Drive or other CEO Network Drives issued to them by IT and should not attempt to access any data or programs contained on CEO's systems for which they do not have explicit consent.
- Users should never access any technical resources using another user's password.
- Unauthorized review, duplication, dissemination, removal, installation, damage, or alteration of files, passwords, computer systems or programs, or other property of the Company, or improper use of information obtained by unauthorized means, is prohibited.
- Users should not divulge any accessed information to anyone not specifically authorized to receive such information
- When accessing CEO's network remotely, users should only do so via CEO's approved virtual private network (VPN).
- Users should not share their CEO authentication information including:
    - Network Passwords
    - Other software passwords
    - Access cards
- Any lost or stolen access cards or keys should be reported to IT as soon as possible.

Authentication/Passwords:

Password control and password policy are of high importance. Passwords allow/deny access to network resources. This can include access to files/folders/PCs/Laptops/Printers etc. The password policy for access to the network must meet the following requirement (which applies to all user accounts):

- Password must meet complexity requirements:
    - At least 12 characters
    - At least 1 lower case
    - At least 1 upper case
    - At least 1 number
    - At least 1 special character
- Maximum age of passwords: 60 Days
- Users cannot reuse 3 of the previous passwords
- If password is entered incorrectly 3 times the user is locked out for a minimum of 15 minutes
- If password is entered incorrectly 5 times, the account will lock automatically and disable for security purposes to ensure that there is no guessing of passwords from an unauthorized individual
- User accounts can only be unlocked by contacting IT.

There is absolutely no need to share password details with anyone other than with a member of the IT Department; this is to ensure that they can support you operationally. Any passwords passed to IT will be kept under the strictest confidence. IT reserve the right to requests any user's password at any stage to ensure network compatibility, integrity and security and operational needs, even if a user is using a personal password. Users are entitled to change their passwords at any time by pressing CTRL+ALT+DLT on their keyboard and select "Change Password" and as long as the password policy requirements are met.

Clear Screen:

- Users should log off from applications or network services and lock their workstations of laptops when they are no longer using them of will be leaving the workspace unattended for a period of time.
- If a user is stepping away from their computer briefly, they should minimize any open screens.
- If a user is serving a customer that could see their computer screen, a privacy screen should be used.
- Copies of documents containing confidential information should be immediately removed form printers and fax machines.
- Staff should not leave customers unattended in their office space at any time.

Data Security:

Agency staff are required to maintain compliance with the NY SHIELD Act and must take reasonable safeguards to protect the security, confidentiality and integrity of sensitive and/or private data.

Safeguards include but are not limited to:

- Users will not, under any circumstances without the specific, prior written authorization of IT Administrator, cause or allow Confidential Information to be saved and/or stored on a computer, drive, device, server, or other digital and cloud based means of data storage (expressly including without limitation Dropbox, OneDrive, Google Drive and Box) other than those in which CEO maintains, controls and provides user secured access.
- Users should use approved encrypted communications methods whenever sending confidential information over public computer networks (sending):
    - Faxed communication should be transmitted via eFax which is encrypted in transit, and stored in an encrypted portal at rest.
    - Emailed communication containing sensitive data will be automatically encrypted via CEO's ZIX encryption software paired with the Microsoft Exchange server. When in doubt, staff should manually encrypt their emails by typing "encrypt" in the subject line.
- When scanning sensitive information, users should utilize a scanner that allows them to scan directly to their desktop or folder and then file and save the information in a secure database or on CEO's network.
- Sensitive data should be stored on CEO's MFA protected network folders.
- All electronic media containing confidential or sensitive information must be securely disposed of after entering it into a data base or moving it to a secure network folder.

Email and Electronic Communication:

- Users are responsible for the accounts assigned to them and for the actions taken on those accounts.

- Accounts access must not be shared without prior authorization from IT, with the exception of calendars and related calendaring functions.
- Staff should not use personal email accounts to send or receive CEO information and correspondence.
- Any personal use of CEO-provided email should not:
    - Involve solicitation for non-CEO business or for personal gain.
    - Be associated with any political entity
    - Forward chain emails.
    - Contain or promote unethical behavior.
    - Violate applicable law or regulation.
    - Result in unauthorized disclosure of CEO **confidential information**.

- Users are expected to use caution when responding to, clicking on links within, or opening attachments included in electronic communications.

- Users shall not send e-mail or other communications that either mask their identity or indicate that they were sent by someone else.

Hardware and Software:

- All employees provided with CEO's Technology Resources, including laptops, iPads or other portable devices, are responsible for the physical security of the resource at all times. All CEO-provided laptops and portable devices are company property.

- Users must promptly report to IT the

    - theft or loss of CEO Technology Resources or

    - unauthorized disclosure of CEO confidential or internal information.

- If a CEO Technology Resource, such as a laptop or portable device, is taken off-site, it must be physically secured at all times.

- CEO strictly prohibits the use of any unapproved hardware or software on its systems, including any hardware or software that is not purchased, installed, configured, tracked, and managed by CEO. Users must not:

    - Install, attach, connect, remove or disconnect, hardware of any kind, including wireless access points, storage devices, and peripherals (i.e. keyboards, mice or similar), to any organizational information system without the knowledge and permission of CEO IT

    - Download, install, disable, remove or uninstall software of any kind, including patches of existing software, to CEO Technology Resources without the knowledge and permission of CEO IT.

- Head Start employees must be aware of and responsible for securing all CEO Technology Resources, including classroom laptops and iPads and portable devices, they have been issued. Head Start employees must be ever mindful of where the device is kept and ultimately its security at all times.

- Head Start laptops and iPads are primarily for classroom use only and must be returned at the end of each day to the designated mobile charging and lock cabinet for iPads and classroom laptops. Classroom laptops and iPads should only be removed from its secure location by the employee it is assigned to, a manger/supervisor, or member of CEO's IT Staff.

- Head Start Managers are responsible for establishing and implementing security procedures for all CEO Technology Resources assigned to their building. Any Technology Resource, including classroom laptops, iPads and portable devices, that will not be used for a considerable amount of time must be locked out of sight in the designated secure cabinet the device is assigned.

Users may not alter or change any security or configuration settings on any CEO Technology Resource without prior approval from ***IT.***

Removable Media

- The use of personal flash drives or other **removable media** must be approved by CEO IT prior to use.
- The use of **removable media** for storage of CEO information must be supported by a reasonable business case.
- **Personally-owned removable media** use is not permitted for storage of CEO information.
- Staff are not permitted to connect **removable media** from an unknown origin without prior approval from CEO IT.
- Confidential and internal CEO information shall not be stored on **removable media** without the use of encryption.
- The loss or theft of a **removable media** device that may have contained CEO information must be reported to the CEO IT immediately.

Security Training and Awareness

- All new staff must complete an approved security awareness training class prior to, or at least within 30 days of, being granted access to any CEO **Resources**.
- All staff must be provided with and acknowledge they have received and agree to adhere to the CEO Information Security Policies before they are granted to access to CEO **Resources**.
- All staff must complete the annual security awareness training.

Copyrighted Materials

- Employees shall not copy and distribute copyrighted material (e.g., software, database files, documentation, articles, graphics files, and downloaded information) through the e-mail system or by any other means unless they have confirmed in advance from IT Administrator that CEO has the right to copy or distribute the material.

- Failure to observe a copyright may result in disciplinary action by CEO as well as legal action by the copyright owner. Any questions concerning these rights should be directed

Voicemail

- Staff should use discretion in disclosing **confidential** or **internal information** in voicemail greetings, such as employment data, internal telephone numbers, location information or other sensitive data.
- Staff should not access another user's voicemail account unless it has been explicitly authorized.
- Staff should update their voicemail in the event of a scheduled absence to reflect the dates they will not be available.

Internet Access

- CEO's Internet access must only be used for business-related activities. Unapproved activities include, but are not limited to:
    - Recreational games
    - Streaming media
    - Personal social media
    - Accessing or distributing pornographic, sexually oriented or other inappropriate or unprofessional materials
    - Attempting or making unauthorized entry to any network or computer accessible from the Internet
    - Any other activity that violates CEO policy

Incidental Personal Use

- As a convenience to CEO staff, incidental personal use of CEO's Technology **Resources** is permitted when not working. The following restrictions apply:
    - Incidental personal use of CEO's Technology Resources is restricted to CEO approved personnel; it does not extend to family members or other acquaintances.
    - An employee's incidental personal use must not
        - result in direct costs to CEO
        - interfere with their productivity or job performance
        - interfere with any other employee's productivity or performance
        - adversely impact the operation of CEO's Technology Resources
    - No files or documents may be sent or received that may cause legal action against, CEO or its customers.
- Access to the Internet from outside the CEO network using a CEO owned computer outside of work hours must comply with all CEO harassment policies.
- Storage of personal email messages, voice messages, files and documents on CEO's Technology **Resources** must be nominal