POLICY AND PROCEDURE

DEPARTMENT: Information Technology SECTION:	NUMBER:	IT-1101
TITLE: **COREConnect Acceptable Use Policy**	ORIGINATED:	9/7/2022
	REVISED:	5/24/2023
	REVIEWED:	5/24/2023

APPROVALS

Owner: Sr. Director of Technology Approved by: Sr Director of Technology Date:	Signature: Approved by: President and COO Date:	Approved by: Date:

Signed Policy can be provided on request to coreconnect@coreresponse.org

I. PURPOSE

It is the purpose of this policy of CORE Community Organized Relief Effort ("CORE") to help ensure the security of 1) any systems under the CORE's direct management control use in connection with COREConnect, 2) any systems not under the CORE's direct management control used in connection with COREConnect and the integrity of Protected Information by clearly defining the acceptable uses of CORE's IT systems use in connection with COREConnect by staff members and contractors. Adherence to this Policy will help CORE guard against internal and external attacks that deny authorized access or result in the loss, dissemination, or compromise of Protected Information in CORE's possession.

II. SCOPE

CORE's IT systems used in connection with COREConnect represent a significant financial asset and is integral to CORE's operations. All data, in any form, created or stored on or transmitted through CORE's IT system, is the property of CORE. Therefore, any document, file or data, whether in the form of text, audio, video, image or photo, or any email, voicemail or other message composed, sent, received, forwarded or stored on or passing through CORE's IT system is the property of CORE and is subject to this Policy.

III. KEY DEFINITIONS

1. **IT System** –
   - **a.** Any and all computer and network infrastructure provided and/or maintained by CORE and used in connection with COREConnect, including desktop and laptop workstations, servers, routers, switches, hubs, firewalls, peripherals, electronic storage devices and related media, PDAs, printers, copiers, scanners, audio/video equipment and all similar devices, whether or not they are attached to CORE's network;

   - **b.** Any and all software applications (purchased or leased) and installed on CORE's computer IT system used in connection with COREConnect; Internet resources, including CORE's web site, email system, intranet(s) or extranet(s); and
   - **c.** Any third-party IT system accessed by or through CORE's IT system use in connection with COREConnect (for example, a personal e-mail account on Yahoo! accessed through CORE's IT system is covered by this Policy).
   - **d.** Any IT system used in connection with COREConnect containing Protected Data used by CORE's Workforce in the course of business.

2. **Protected Information** – Personal Data and Protected Health Information.
3. **Personal Data** – Any information relating to an identified or identifiable natural person (Data Subject); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person. Personal Data includes Special Categories of Personal Data and pseudonymized Personal Data but excludes anonymous data or data that has had the identity of an individual permanently removed. Personal Data can be factual (for example, a name, email address, location or date of birth) or an opinion about that individual's actions or behavior.
4. **Special Categories of Personal Data** – Personal Data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade-union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation.

IV. REASONS FOR ACCEPTABLE USE POLICY

It is the purpose of this Policy to provide CORE's staff members with guidelines regarding acceptable uses of 1) any systems under CORE's direct management control used in connection with COREConnect and 2) any systems not under CORE's direct management control used in connection with COREConnect, in order to avoid compromising the integrity of the IT systems used in connection with COREConnect by inadvertent exposure to malicious software and other external attacks. This Policy also sets forth procedures for detecting and reporting malicious software. This Policy applies to all staff members of CORE involved with COREConnect.

V. USING THE IT SYSTEM APPROPRIATELY

1. General Rules. Staff members will follow these rules when using 1) any systems under CORE's direct management control used in connection with COREConnect, and 2) any systems not under CORE's direct management control used in connection with COREConnect, unless otherwise authorized by the Security Officer or any executive officer of CORE:

   a. Do not use peer-to-peer file sharing programs.;

   b. Do not download free programs offered on the Internet, including "free" anti-virus software;

   c. Do not click on pop-ups, including those that purport to fix a "problem" with the computer;

   d. Do not defeat nor disable any security features at a workstation or on a portable device;

   e. Do not access, or attempt to access, the directories of other staff members or any documents, emails files or other similar items that are addressed to other staff members without specific authorization;

   f. Do not access websites, or generate, store or forward email or voicemail or files (including images, text, audio, video, etc.) which contain offensive, threatening or disruptive materials;

g. Do not gain unauthorized access to others' networks or IT system (frequently referred to as "hacking") to access content that is the intellectual property, copyrighted material and/or trade secrets of another organization;

h. Do not use another person's account or an alias to access the IT system and/or external networks or systems;

i. Do not generate or transmit any material, in any form, that offensively addresses someone's age, sexual orientation, religious or political beliefs, national origin or disability;

j. Do not generate bulk messages (frequently known as "SPAM"), or facilitate pyramid marketing, chain letters or the promotion of hoaxes; and

k.Do not conduct any activity on the IT system not specifically in furtherance of your job responsibilities for CORE.

2. Email Use. Staff members should restrict email usage to that which is required to complete the staff member's job responsibilities. Staff members should not assume confidentiality of messages transmitted via email or over the Internet on CORE's IT systems used in connection with COREConnect. CORE reserves the right to monitor and/or inspect any employee's email usage. Staff members will not put CORE's authorization codes, credit card numbers, or similar items in email messages without the prior authorization of the Security Officer or an executive officer of CORE.

3. Internet Use. Staff members should restrict Internet use to business purposes only during working hours. Any employee that violates this policy may be subject to disciplinary action, up to and including termination.

4. Installation of Hardware and Software. To prevent the introduction of malicious code and protect the integrity of CORE's IT system, staff members will obtain all hardware and software from CORE. Staff members may not install software without prior approval of the Security Officer or the Director, Information Technology.

5. Software Licenses. Some software used on CORE's IT system used in connection with COREConnect is licensed and/or registered in the name of CORE. Staff members will abide by software copyright laws and will not obtain, install, duplicate or use software except as permitted by CORE's software licensing agreements.

VI. DETECTING AND REPORTING SUSPICIOUS EVENTS

1. If a staff member experiences any of the following events that may indicate the presence of malicious software and/or a security incident, the staff member will report it to the Security Officer and/or any executive officer of CORE:

a. anti-virus software alerts regarding a virus, worm or other malicious code attack;

b. persistent intrusion attempts from any entity;

c. system slowdown;

d. data loss on one or more workstations, on the server(s) or on any hard drive or back-up tape;

e. server crash;

f. receipt of threatening email messages;

g. large number of bounced emails with suspicious content;

h. auditing configuration change in log;

i. log entries showing use of a Web vulnerability scanner;

j. a workstation, laptop or server processor whose CPU utilization is noticed to be abnormally high (e.g., 90% or more) for an extended period of time (more than a few minutes);

k. a change in user accounts (e.g., addition, deletion or modification of access rights or profiles;

l. absence of incoming or outgoing emails for an abnormally long period of time;

m. the unusual appearance of any new file, directory, software, icon, toolbar, shortcut, desktop wallpaper or screensaver;

n. any sudden or unusual problems with logging in using the normal ID and password;

o. the appearance of an unknown or unrecognized username or user log-in screen, other than what is normally expected;

p. the sudden change of your internet “home page,” or a scenario where multiple browser windows seem to open up on their own; or

q. any situation where you think someone’s user ID or password might have been compromised or shared with someone.

2. Staff members are encouraged to make good faith reports to the Security Officer and/or any executive officer of CORE regarding any instance in which they observe the inadvertent or intentional violation of this policy by other staff members. Staff members are also encouraged to self-report their own inadvertent violations of this Policy. The nature of the violation, the degree of harm caused by the violation and the cooperation of the staff member will be considered in determining the type of sanction, if any, which will be imposed for any violation of this Policy. All reports should be submitted via CORE’s Incident Report Form, available through CORE’s Intranet home page, by clicking on “Reporting and Requests” and then “Security/Safety Incident”.

3. The Security Officer or designee(s) will investigate the event in accordance with applicable policies regarding security incident reporting and response. CORE reserves and intends to exercise the right to review, audit, intercept, and access all data without the permission of the staff member on any workstation or CORE provided portable device.