Security Awareness and Acceptable Use Policy

Overview

Centric Consulting ("Centric") is committed to protecting all Associates, clients, and the company from illegal or damaging actions by individuals, either knowingly or unknowingly. The intention of this Security Awareness and Acceptable Use Policy is to help protect our Associates and clients without imposing restrictions that are contrary to the established culture of openness, trust, and integrity.

Effective security is a team effort requiring the participation and support of every Centric Associate who deals with information and/or information systems. It is the responsibility of every user to know these guidelines, and to conduct their activities accordingly.

Scope

This policy applies to employees, contractors, consultants, temporary employees, and all other workers at Centric, including all personnel affiliated with third-parties ("Associates"). This policy also applies to the use of all computer equipment, mobile devices, networks, software and services owned or leased by Centric, or used to conduct business on behalf of Centric even if not owned or leased by Centric ("Platforms").

Policy

General Use and Ownership

1. Associates should be aware that any content or deliverables created, modified or adapted on corporate Platforms remains the property of Centric.
2. While Centric IT desires to provide a reasonable level of privacy, it also has the responsibility of managing and securing devices, applications and services used for Centric business purposes. As a result of the access required to meet these responsibilities, Centric cannot guarantee the confidentiality of Associate personal information or data stored or transmitted on these Platforms from personnel within Centric IT.
3. Associates should understand and adhere to both Centric and client policies on acceptable use. Where policies overlap, the more restrictive policy should be followed. Individuals are responsible for exercising good judgment regarding reasonable acceptable use in relation to those policies. Centric leadership or Centric IT should be consulted if there is any uncertainty.
4. Public computers, such as those in hotel or airport business centers should not be used for Centric business.
5. Any information considered sensitive must be encrypted when stored, transmitted, or otherwise shared. For example, share a link to a sensitive file stored in a secure location such as OneDrive, rather than sending as an email attachment. If there is any doubt whether information should be considered 'sensitive', err on the side of caution and treat it as such, or consult with Centric IT.
6. To properly manage Centric's Platforms, authorized individuals within Centric IT may monitor equipment, systems, and network traffic at any time.
7. Centric reserves the right to audit Centric's Platforms on a periodic basis to ensure compliance with Centric policies.

8. Associates will not remove or otherwise tamper with the security and monitoring software and settings configured by Centric IT. This includes but is not limited to whole disk encryption, anti-virus software, OS policy settings and system monitoring and remote support software.

Security and Proprietary Information

1. Client, or client customer data that is regulated by data protection standards including but not limited to HIPAA, PCI or PII ("Regulated Data") should not be stored or processed on Centric Platforms, nor personal devices. Client work involving data of this nature must be performed on client provided computers, or via a client secured remote virtual desktop or browser connection for access to client data systems. Associates may be liable if security of regulated data is compromised due to actions, inactions or omissions by the Associate or by an Associate under their supervision. Exceptions to this policy must be approved by a Managing Member.
2. Associates are required to be aware of and abide by any and all applicable client information security policies and should take all necessary steps to prevent unauthorized access to data owned by Centric or Centric's clients.
3. All Centric and personal devices used for Centric business must be secured with a password-protected device lock or screen saver with the automatic activation feature enabled.
4. Associates should not use their Centric email address to post to online services or social media, unless posting is in the course of business duties and is not detrimental to Centric's business concerns.
5. Any computer used to conduct Centric business must always be actively running approved virus-scanning software with a current virus database.
6. Associates must use extreme caution when opening email attachments or clicking emailed links. Any uncertainty is an indication that it should NOT be opened and should be reported to Centric IT.

Unacceptable Use

Under no circumstances is an Associate of Centric authorized to engage in any activity that is illegal under local, state, federal, or international law.

Additionally, the following activities are generally prohibited. Associates may be exempted from these restrictions during the course of their legitimate job responsibilities with approval from Centric IT.

1. Automated forwarding calendar details or email from an individual's Centric mail/calendar account to a client mail/calendar account. This can result in the leakage of information sensitive to Centric or other Centric clients. Manual forwarding of email or calendar appointments to a client account is permitted only when the content does not contain information related to any other clients.
2. Providing information about, or lists of, Centric or client data to parties outside of Centric.
3. Revealing your account password to others or allowing use of your account by others. Associates are responsible for the security of their passwords and accounts.
4. Sending, forwarding, or requesting email with any type of Regulated Data. If there is any doubt whether content should be considered Regulated Data, treat it as such and obtain guidance from Centric IT.
5. Sending or forwarding email that may contain malware.

6. Sending unsolicited email messages, including the sending of "junk mail" or other advertising material to individuals who did not specifically request such material (email spam) unless in execution of Centric official marketing initiatives.
7. Using a Centric or client computing asset to actively engage in procuring or transmitting material that is in violation of sexual harassment or hostile workplace laws.
8. Performing any action that interferes with or denies a Centric Associate's ability to legitimately use Centric's Platforms and property.
9. Introduction of malware of any type into Centric's or client Platforms.
10. Connecting networking equipment (i.e. wireless access points, routers, etc.) into the Centric network environment without proper authorization from the Centric IT.
11. Effecting security breaches, disruptions, scanning, monitoring or otherwise tampering with network communications.
12. Bypassing the login process or other security measures of any device, network, or account.
13. Exporting software, technical information, encryption software, or technology, in violation of international or regional export control laws, is illegal. Centric IT should be consulted prior to export of any material that is in question.
14. Making fraudulent offers of products, items, or services originating from any Centric account.
15. Making statements about warranty, expressly or implied, unless it is a part of normal job duties.

Disciplinary Consequences

Any Associate found to have violated this policy may be subject to disciplinary action, up to and including termination of employment or services.