ACCEPTABLE USE POLICY

NextGen CGI, LLC

Document Owner: NextGen CGI, LLC
Effective Date: January 1, 2021
Updated:

NextGen CGI, LLC Acceptable Use Policy							
Effective Date:		January 1, 2021		**Document Owner:**		NextGen CGI, LLC	
Revision History							
Revision	Rev. Date	Description	Prepared By	Reviewed By	Date	Approved By	Date
1.0	01/01/2021		S. Hall	S. Hall	01/01/2021	S. Hall	01/01/2021

1. Overview

Effective security is a team effort involving the participation and support of every NextGen CGI IT support specialist and affiliate who deals with information and/or information systems. It is the responsibility of every computer user to know these guidelines, and to conduct their activities accordingly.

2. Purpose

The purpose of this policy is to outline the acceptable use of computer equipment at NextGen CGI. These rules are in place to protect the IT support specialist and NextGen CGI. Inappropriate use exposes NextGen CGI to risks including virus attacks, compromise of network systems and services, and legal issues.

3. Scope

This policy applies to the use of information, electronic and computing devices, and network resources to conduct NextGen CGI business or interact with internal networks and business systems, whether owned or leased by NextGen CGI, the IT support specialist, or a third party. All IT support specialists, contractors, consultants, temporary, and other workers at NextGen CGI and its subsidiaries are responsible for exercising good judgment regarding appropriate use of information, electronic devices, and network resources in accordance with NextGen CGI policies and standards, and local laws and regulation. Exceptions to this policy are documented in section 5.2.

This policy applies to IT support specialists, contractors, consultants, temporaries, and other workers at NextGen CGI, including all personnel affiliated with third parties. This policy applies to all equipment that is owned or leased by NextGen CGI.

4. Policy

4.1 General Use and Ownership

4.1.1 NextGen CGI proprietary information stored on electronic and computing devices whether owned or leased by NextGen CGI, the IT support specialist or a third party, remains the sole property of NextGen CGI. You must ensure through legal or technical means that proprietary information is protected in accordance with the *Data Protection Standard.*

4.1.2 You have a responsibility to promptly report the theft, loss or unauthorized disclosure of NextGen CGI proprietary information.

4.1.3 You may access, use or share NextGen CGI proprietary information only to the extent it is authorized and necessary to fulfill your assigned job duties.

4.1.4 IT support specialists are responsible for exercising good judgment regarding the reasonableness of personal use. Individual departments are responsible for creating guidelines concerning personal use of Internet/Intranet/Extranet systems. In the absence of such policies, IT support specialists should be guided by departmental policies on personal use, and if there is any uncertainty, IT support specialists should consult their supervisor or manager.

4.1.5 For security and network maintenance purposes, authorized individuals within NextGen CGI may monitor equipment, systems and network traffic at any time, per NextGen CGI's *Audit Policy*.

4.1.6 NextGen CGI reserves the right to audit networks and systems on a periodic basis to ensure compliance with this policy.

4.2 Security & Proprietary Information

4.2.1 All mobile and computing devices that connect to the internal network must comply with the *Minimum Access Policy*.

4.2.2 System level and user level passwords must comply with the *Password Policy*. Providing access to another individual, either deliberately or through failure to secure its access, is prohibited.

4.2.3 All computing devices must be secured with a password-protected screensaver with the automatic activation feature set to 10 minutes or less. The screen must be locked or log off when the device is unattended.

4.2.4 Postings by IT support specialists from a NextGen CGI email address to newsgroups should contain a disclaimer stating that the opinions expressed are strictly their own and not necessarily those of NextGen CGI, unless posting is in the course of business duties.

4.2.5 IT support specialists must use extreme caution when opening e-mail attachments received from unknown senders, as they may contain malware.

4.3 Unacceptable Use

The following activities are, in general, prohibited. IT support specialists may be exempted from these restrictions during the course of their legitimate job responsibilities (e.g., systems administration staff may have a need to disable the network access of a host if that host is disrupting production services).

Under no circumstances is an IT support specialist of NextGen CGI authorized to engage in any activity that is illegal under local, state, federal or international law while utilizing NextGen CGI-owned resources.

The lists below are by no means exhaustive, but attempt to provide a framework for activities which fall into the category of unacceptable use.

4.3.1 System and Network Activities

The following activities are strictly prohibited, with no exceptions:

1. Violations of the rights of any person or company protected by copyright, trade secret, patent or other intellectual property, or similar laws or regulations, including, but not limited to, the installation or distribution of "pirated" or other software products that are not appropriately licensed for use by NextGen CGI.

2. Unauthorized copying of copyrighted material including, but not limited to, digitization and distribution of photographs from magazines, books or other copyrighted sources, copyrighted music, and the installation of any copyrighted software for which NextGen CGI or the end user does not have an active license is strictly prohibited.

3. Accessing data, a server or an account for any purpose other than conducting NextGen CGI business, even if you have authorized access, is prohibited.

4. Exporting software, technical information, encryption software or technology, in violation of international or regional export control laws, is illegal. The appropriate management should be consulted prior to export of any material that is in question.

5. Introduction of malicious programs into the network or server (e.g., viruses, worms, Trojan horses, e-mail bombs, etc.).

6. Revealing your account password to others or allowing use of your account by others. This includes family and other household members when work is being done at home.

7. Using a NextGen CGI computing asset to actively engage in procuring or transmitting material that is in violation of sexual harassment or hostile workplace laws in the user's local jurisdiction.

8. Making fraudulent offers of products, items, or services originating from any NextGen CGI account.

9. Making statements about warranty, expressly or implied, unless it is a part of normal job duties.

10. Effecting security breaches or disruptions of network communication. Security breaches include, but are not limited to, accessing data of which the IT support specialist is not an intended recipient or logging into a server or account that the IT support specialist is not expressly authorized to access, unless these duties are within the scope of regular duties. For purposes of this section, "disruption"

includes, but is not limited to, network sniffing, pinged floods, packet spoofing, denial of service, and forged routing information for malicious purposes.

11. Port scanning or security scanning is expressly prohibited unless prior notification to NextGen CGI is made.
12. Executing any form of network monitoring which will intercept data not intended for the IT support specialist's host, unless this activity is a part of the IT support specialist's normal job/duty.
13. Circumventing user authentication or security of any host, network or account.
14. Introducing honeypots, honeynets, or similar technology on the NextGen CGI network.
15. Interfering with or denying service to any user other than the IT support specialist's host (for example, denial of service attack).
16. Using any program/script/command, or sending messages of any kind, with the intent to interfere with, or disable, a user's terminal session, via any means, locally or via the Internet/Intranet/Extranet.
    i. Providing information about, or lists of, NextGen CGI IT support specialists to parties outside NextGen CGI.
17. Providing information about, or lists of, NextGen CGI IT support specialists to parties outside NextGen CGI.

4.3.2 Email and Communication Activities

When using company resources to access and use the Internet, users must realize they represent the company. Whenever IT support specialists state an affiliation to the company, they must also clearly indicate that "the opinions expressed are my own and not necessarily those of the company". Questions may be addressed to the IT Department

1. 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).
2. Any form of harassment via email, telephone or paging, whether through language, frequency, or size of messages.
3. Unauthorized use, or forging, of email header information.
4. Solicitation of email for any other email address, other than that of the poster's account, with the intent to harass or to collect replies.

5. Creating or forwarding "chain letters", "Ponzi" or other "pyramid" schemes of any type.

6. Use of unsolicited email originating from within NextGen CGI's networks of other Internet/Intranet/Extranet service providers on behalf of, or to advertise, any service hosted by NextGen CGI or connected via NextGen CGI's network.

7. Posting the same or similar non-business-related messages to large numbers of Usenet newsgroups (newsgroup spam).

4.3.2 Blogging and Social Media

1. Blogging by IT support specialists, whether using NextGen CGI's property and systems or personal computer systems, is also subject to the terms and restrictions set forth in this Policy. Limited and occasional use of NextGen CGI's systems to engage in blogging is acceptable, provided that it is done in a professional and responsible manner, does not otherwise violate NextGen CGI's policy, is not detrimental to NextGen CGI's best interests, and does not interfere with an IT support specialist's regular work duties. Blogging from NextGen CGI's systems is also subject to monitoring.

2. NextGen CGI's Confidential Information policy also applies to blogging. As such, IT support specialists are prohibited from revealing any NextGen CGI confidential or proprietary information, trade secrets or any other material covered by NextGen CGI's Confidential Information policy when engaged in blogging.

3. IT support specialists shall not engage in any blogging that may harm or tarnish the image, reputation and/or goodwill of NextGen CGI and/or any of its IT support specialists. IT support specialists are also prohibited from making any discriminatory, disparaging, defamatory or harassing comments when blogging or otherwise engaging in any conduct prohibited by NextGen CGI's *Non-Discrimination and Anti-Harassment* policy.

4. IT support specialists may also not attribute personal statements, opinions or beliefs to NextGen CGI when engaged in blogging. If an IT support specialist is expressing his or her beliefs and/or opinions in blogs, the IT support specialist may not, expressly or implicitly, represent themselves as an IT support specialist or representative of NextGen CGI. IT support specialists assume any and all risk associated with blogging.

5. Apart from following all laws pertaining to the handling and disclosure of copyrighted or export controlled materials, NextGen CGI's trademarks, logos and any other NextGen CGI intellectual property may also not be used in connection with any blogging activity

5. Policy Compliance

5.1 Compliance Measurement

The NextGen CGI team will verify compliance to this policy through various methods, including but not limited to, business tool reports, internal and external audits, and feedback to the policy owner.

5.2 Exceptions

Any exception to the policy must be approved by the NextGen CGI team in advance.

5.3 Non-Compliance

An IT support specialist found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

6. Related Standards, Policies, and Processes

- Data Classification Policy
- Data Protection Standard
- Social Media Policy
- Minimum Access Policy
- Password Policy

7. Definitions and Terms

The following definitions are not all-inclusive and should be updated as new information is made available:

RESTRICTED