CHOICE FINANCIAL GROUP

CHOICE FINANCIAL GROUP
CONTRACTOR ACCEPTABLE USE AGREEMENT

Choice Financial Group ("CFG") and Rohan Srivastwa _____ ("Contractor") enter into this Acceptable Use Agreement ("Agreement") to set forth the terms under which Contractor will have access to CFG's technology systems and information. Together, CFG and Contractor are referred to herein as "the Parties."

1. Purpose. The purpose of this Agreement is to assure that all parties with access to CFG information and/or systems comply with expected acceptable and restricted use. Contractor understands and agrees that through the use of CFG's information and/or systems, Contractor has access to confidential business and customer information. CFG and Contractor are subject to banking regulations and other laws and regulations that require the parties to retain customer information confidentially. Further, through CFG's technology system, Contractor has access to CFG's confidential and proprietary information. By entering into this Agreement, the Parties seek to protect business and customer information and set forth the terms under which Contractor has access to such information.

2. Access. In exchange for Contractor's agreement to the terms of this Agreement, CFG will provide Contractor access to its technology, and as appropriate and legal, to customer information. This means that Contractor may have access to a variety of confidential, internal, and public information during the course of business. The Parties agree that this access, and the ability to conduct business with CFG's customers, is sufficient consideration for the terms and conditions of this Agreement.

3. Confidentiality and Non-Disclosure. Information is classified in a level of confidentiality, based on a specific secrecy and protection that must be granted to such information. Unauthorized disclosure or misuse of confidential or customer information is strictly prohibited. Contractor will not, for any reason, use such information for non-business or personal use – regardless of whether the information is confidential, internal, or public. Contractor further agrees to ensure the confidentiality of customer information by not disclosing information to any entity or individual (whether or not a CFG employee) that does not have a business-need and right to the access of such information.

4. Usage of CFG's Internet Services, Technology and Information. All information systems and communications, including internet connectivity and e-mail, are property of CFG. Contractor agrees to use CFG's internet services, technology and information only for Acceptable Activities. At no time will Contractor use CFG's resources for Prohibited Activities or for any other illegal activities, including but not limited to activities related to violence, harassment, obscenity.

5. Acceptable Activities. For purposes of this Agreement, the following activities are Acceptable Activities:

- Using information technology systems to complete the activities specified in Contractor's engagement agreement.

- Using electronic communication to communicate with customers and other employees who have a legitimate business need for and have a right to access the information, to meet operational needs.

- Accessing systems and resources that Contractor has been authorized to use.

- Accessing approved online resources.

6. **Prohibited Activities.** Contractor shall, at no time, unless directly authorized by management, attempt to bypass any security control or access information for which Contractor does not have sufficient privileges. Additionally, at no time shall Contractor perform any Prohibited Activities. For purposes of this Agreement, the following activities are Prohibited Activities:

- Using systems in any way that intentionally or unintentionally violates any applicable local, state, national, or international law or any rules or regulations published under the terms or authority of such laws.

- Attempting to break into accounts, crack passwords, or disrupt any services.

- Attempting to access systems to which Contractor knows Contractor does not have access.

- Using electronic communications to engage in any communications or action considered to be threatening, illegally discriminatory or harassing, defamatory, slanderous, or obscene.

- Using electronic communications to make fraudulent offers to sell or buy products, items, or services or to advance any type of financial scam such as "pyramid schemes," "Ponzi schemes," and "chain letters."

- Adding, removing, or modifying identifying information in an attempt to deceive or mislead or attempt to impersonate any person other than Contractor's true identity.

- Using systems to access (or to attempt to access) the accounts of others, or to penetrate (or attempt to penetrate) security measures of CFG's or another entity's computer software or hardware, electronic communications system, or telecommunications system, whether or not the intrusion results in the corruption or loss of data.

- Using systems for any activity that adversely affects the ability of other people or systems to use CFG systems. This includes a Denial of Service (DoS) attack, spreading malicious software, and excessive use of computing or network resources.

- Downloading or installing any unapproved software without the authorization of CFG's IT Team.

- Visiting unapproved websites or website content that is not directly related to engagement agreement responsibilities.

- Introducing any unapproved CD's, floppy disks, USB devices, or other media/hardware to any CFG system.

- Opening unknown attachments to electronic mail. Contractor understands that users should never, under any circumstances, open email attachments from unknown parties or those of a suspicious nature.

- Using email or other electronic communications to transmit unencrypted, internal, or confidential information, or files that are not for business use or for malicious purposes.

- Revealing or publicizing confidential or proprietary information, which includes, but is not limited to, financial information, confidential client information, marketing strategies and plans, databases and any information contained within these systems, client lists, computer software source codes, computer/network access codes, and business relationships.

- Copying software or media, for any reason, that has been purchased, developed, or is owned by CFG, without prior authorization.

- Altering the network infrastructure without prior authorization and proper instruction. The network infrastructure consists of and is not limited to workstations, servers, wiring, switches, hubs, routers, firewalls, wireless devices, modems, internet connections, phone lines, and power connections.

- Altering or disabling malicious software protection programs unless prior authorization is received. Contractor shall report any suspicious or actual malicious software activity immediately to the CFG Information Security Officer.

7. Username and Password Responsibilities. When appropriate and necessary, Contractor will be provided credentials to CFG information systems. Contractor shall never share Contractor's usernames and passwords with anyone for any reason. Contractor understands and agrees that Contractor is responsible to build the strongest possible password allowably by the system and Contractor will be accountable for failing to meet password standards. Contractor also understands and agrees Contractor is responsible and will be held accountable for any actions taken with their credentials, including any liability caused in whole or in part by Contractor's conduct or failure to protect the information.

8. Collection of Private Data and Monitoring. Contractor agrees that the information systems are property of CFG and are to be used for business purposes only. Contractor understands that Contractor's activities may be monitored and data on these systems may be collected. Contractor has no expectation of privacy when using CFG systems. Contractor also understands and agrees that CFG has the right to monitor, access, review, copy, store, or delete any electronic communications,

including personal messages, from its systems for any purpose and to disclose them to others as deemed appropriate.

9. Contractor Responsibilities regarding Security. Contractor will take all the necessary precautions to protect CFG assets and information. This includes the proper use of information systems, protection of usernames and passwords, keeping sensitive information clear of desk and screen, proper disposal of sensitive information, and reporting security weaknesses and incidences including violations to company policies.

Contractor shall secure all removable media (e.g., floppy disks, zip disks, tapes, and compact discs) in some manner. This means controlling access in such a way that unauthorized access by anyone cannot be accomplished. This includes blank media, software media, and data media. Contractor shall also ensure that sensitive documentation is stored in a secure location. Contractor shall not leave confidential documentation, sensitive documentation, or storage media devices containing such documentation in Contractor's work areas during non-business hours or unattended for extended lengths of time during business hours.

Contractor shall not leave confidential or sensitive information displayed on computer screens when screens are not supervised. Proper monitor placement prevents the discloser of confidential and sensitive information to customers or employees within the facility. Therefore, Contractor shall position Contractor's computer display screen(s) to prevent viewing from public areas and from externally facing windows when possible. Additionally, before leaving a workstation unattended, Contractors shall log off or lock system.

10. Remote Access/VPN Use. Contractor will be allowed to access CFG's VPN when there is a distinct business need for the VPN access. All computers connected to the CFG network via VPN will be CFG owned/controlled computers, with up-to-date security patches and anti-virus software. When connected to the CFG network via VPN, Contractor agrees that the same acceptable use rules apply as if Contractor were physically on-site, including but not limited to rules such as clear desk and clear screen, document disposal, notification of a potential security breach, and loss or damage of CFG equipment.

11. Reporting a Violation of the Acceptable Use Agreement or Security Issue. Contractor shall report any incident or suspected incident of unauthorized access and/or disclosure of company data immediately to the CFG Information Security Officer, the CFG IT Team, or a member of the management team. Contractor shall immediately report any possible or actual security weaknesses and incidents that Contractor becomes aware of to the CFG Information Security Officer.

12. Maintaining Virus Protection Software on Each Computer. Contractor shall alert the CFG IT Team when any failure or virus message occurs. If such an event does occur, Contractor will do the following:

- Do not turn off the computer.
- Immediately make detailed notes regarding failure. The circumstances leading to the failure should be noted, and the notes should be dated and signed.
- If an error message is given, the error message should be copied into the notes.

- If a printer is available and functioning, print the screen containing the error message or the screen that will demonstrate the failure.

13. **Full Agreement.** This Agreement contains the full agreement between the Parties regarding Contractor's with access to CFG information and/or systems, including the expected acceptable and restricted use of such information and/or systems. This Agreement may not be modified, altered, or changed in any way except by written agreement signed by both parties, except that CFG may modify the definitions of Acceptable Activities and Prohibited Activities in Sections 5 and 6 of this Agreement with written notice to Contractor. The parties agree that this Agreement supersedes and terminates any and all other written and oral agreements and understandings between the parties regarding the access and acceptable use of CFG's information and/or systems. Notwithstanding the foregoing, if Contractor has previously signed an agreement or agreements with CFG containing confidentiality, trade secret, noncompetition, non-solicitation, inventions, and/or similar provisions, Contractor's obligations under such agreement(s) will continue in full force and effect according to their terms.

14. **Enforcement.** Contractor has read, understands, and voluntarily entered into this Agreement. Contractor agrees that a breach or threatened breach of this Agreement will cause CFG grave and irreparable injury and damage. Accordingly, CFG will be entitled to equitable relief to prevent any such breach, in addition to any other available remedies in law and in equity. If a court finds any term of this Agreement to be invalid, unenforceable, or void, the Parties agree that the court will modify such term to make it enforceable to the maximum extent possible. If the term cannot be modified, the parties agree that the term will be severed, and all other terms of this Agreement will remain in effect.

15. **Law Governing.** This Agreement will be governed and construed in accordance with the laws of the State of North Dakota.

CONTRACTOR	**CHOICE FINANCIAL GROUP**
Rohan Srivastwa	By: Ali Marie Huber
Name	Its: Employee Onboarding and Benefits Specialist
Electronically Signed By Rohan Srivastwa	
Signature	
1/2/2024	1/2/2024
Date	Date