

## Contractor Mobile Device Access Agreement

Choice Financial Group (“CFG”) agrees to provide Rohan Srivastwa (“Contractor”) access to information in CFG’s system through certain, pre-approved mobile devices under certain conditions, through which Contractor will be able to conduct business involving CFG’s customers and clients.

Only after approval by CFG will Contractor’s device(s) be connected to the CFG system. Contractor shall not access the CFG system on any other devices. Further Contractor agrees that Contractor’s access to CFG through Contractor’s device(s) is subject to the following terms;

- All devices used to access the CFG system must use malware prevention software. Contractor is responsible for providing malware prevention software.
- Contractor must promptly install any software updates on the devices used to access the CFG system.
- All devices used to access the CFG system must enforce a screen locking mechanism that requires a password to resume usage.
- Contractor shall not share Contractor’s password(s) on the device(s) used to access the CFG system with anyone, including family and friends.
- Contractor is responsible at all times for providing physical security for the device(s) Contractor uses to access the CFG system.
- Contractor agrees that CFG IT Department is responsible for servicing CFG systems only.
- Contractor shall not circumvent built-in security controls within the devices used to access the CFG system without the approval from the IT team (e.g., jailbreaking an iPhone).
- Smartphones used to access the CFG email system must be enrolled in CFG’s mobile device management solution to allow for remote wiping of CFG corporate data.
- Contractor shall not save CFG data locally to personal device. All data must reside within CFG systems.
- Contractor shall immediately report any incident or suspected incidents of unauthorized access and/or disclosure of CFG resources, information, systems, or other such areas.
- Contractor shall notify the CFG Cybersecurity or IT team of lost, stolen, or soon-to-be retired personal devices.
- Contractor shall not improperly dispose of personal devices that have stored, processed, or transmitted CFG information at any time.
- Contractor agrees that at the termination of Engagement Agreement, all CFG data will be either returned to CFG or destroyed as indicated by CFG at the time of contract termination.

In the event that CFG is required to produce Electronic Discovery or to undergo forensic investigation of electronic information – in criminal or civil litigation, for a governmental agency investigation, or for any other process in which CFG is legally required to produce Electronic Discovery or participate in a forensic investigation – Contractor agrees to provide CFG any devices Contractor has used to access the CFG system immediately upon request. Similarly, if CFG believes it has probable cause to conduct a forensic investigation of the device(s) Contractor has used to access CFG information, Contractor will provide CFG the device(s) immediately upon request. In all of these circumstances, Contractor further agrees that CFG will possess the device(s) until a forensic image can be created and verified for integrity. A comparable replacement device will be offered to Contractor in the event the original device(s) is not returned in a timely manner. Contractor agrees that CFG may outsource any forensic or Electronic Discovery processes to an external third party.

### CONTRACTOR

Rohan Srivastwa

Name

Electronically Signed By

Rohan Srivastwa

Signature

1/2/2024

Date

### CHOICE FINANCIAL GROUP

By: Ali Marie Huber

Its: \_\_\_\_\_

1/2/2024

Date