CLIENT DATA PRIVACY & CONFIDENTIALITY

1) Employees, volunteers, and board members of PCIO are bound by strict standards of conduct when protecting the confidentiality and privacy of our clients. Portable CIO and its employees protects and maintains the confidentiality of all client data, their family members and acquaintances, in the regular course of providing technical services. Our confidentiality policy covers all data a Portable CIO employee may encounter while working on behalf of a client, on their local computer, their network server, telephone, tablet or laptop, hardisk, network storage, etc., regardless of origin or use. There are no exceptions carved to this policy.

2) Confidential communications include conversations, reports, forms, correspondence and all manner of stored electronic information and computer-generated communications with, about or involving in any way any client of PCIO. Minors are entitled to the same confidentiality, and only the guardian of the minor can waive their confidentiality. Internal PCIO access to documentation is limited to an "as needed/need to know" basis for the sole purpose of evaluation, maintenance and repair of client computer systems, software, networking and electronic infrastructure.

PROTECTED CLIENT INFORMATION (PCI)

3) PCI is defined as any data stored on client computer equipment above and beyond the basic operating system or generic programs used to operate the computer. It includes individual documents, customer relationship management data (CRM), license keys, codes, procedures, documents, or methods the client uses to execute their personal or professional duties. This policy includes any secondary client data, e.g., any data our client may safeguard

for their own clients, and unto which they are bound to protect. All data Portable CIO encounters is treated equally, and all is bound by this confidentiality policy.

RESPONSIBILITIES AND OBLIGATIONS

4) PCIO and its employees have a professional and ethical obligation to respect the privacy of our clients, and to protect and maintain the confidentiality of all information that we obtain about clients, their associates, and family members in the course of providing services to them. Portable CIO, Inc's primary goal is not only the protection of the confidentiality of PCI, but protection of the data itself from any alteration or potential risk to its integrity while it is in the care of Portable CIO, Inc., and within the limitations of the state of the hardware and data when it is received for repair. For a full description of the limitations of Portable CIO, Inc's liability with regard to computer equipment and data presented for repair, please see the PCIO 2023 Terms and Conditions.

EXECUTION OF ROUTINE SAFEGUARDS

5) In the course of in-office computer system repair, PCIO technicians may, in their professional discretion to safeguard a client's dataset, create and store a backup image (snapshot) of an entire client computer in order to safeguard the computing environment prior to potentially hazardous repairs, or to safeguard a known-failing computer environment from data loss. Snapshots of client computers, including their PCI are routinely created in cases of a failing disk storage, disk partition adjustments, disk-to-disk cloning, and transitions from old to new computers. Snapshots are not created for routine maintenance unless there is, in the judgment of the involved technician, a risk of data loss given the particular requirements of the situation.

6) Snapshots of client computer systems are stored in a proprietary and compressed whole-disk format on a password protected backup server. Client data snapshots created by PCIO in no way may be considered an absolution of a client's responsibility to maintain regular and thorough backups of their systems and critical datasets. Client data snapshots are only used for the purpose of risk avoidance, and are deleted from PCIO backup servers following the confirmed repair and successful re-integration of client computer systems into the client environment.

7) Ensuring current and complete backups is the responsibility of the computer owner. Client data snapshots are for the sole and express purpose of safeguarding client data from loss during the repair process while computers are under the care and responsibility of PCIO.

CLIENT DATA

8) Portable CIO will not delete customer data under any circumstance. Technicians will, if requested, advise clients on the proper method to navigate and delete data, however those actions must be carried out by the data owner under PCIO advice, *not* by a PCIO technician being observed by a client.

9) PCIO technicians do not require the access (opening and inspection) of individual files containing PCI. PCIO technicians are concerned with the wholesale movement and safeguarding of large amounts of information (files) from system to system, to effect repairs while ensuring the safety and integrity of the aggregate dataset. PCIO technicians have no reason to access client PCI, beyond confirming the veracity of copied/moved data, or examining corrupted disks for data that has been harmed. This is to ensure the successful movement and reintegration of the dataset into a repaired computer environment.

10) PCIO may be asked to manipulate a discreet dataset. For example, the breaking up of an extremely large Outlook PST file into smaller accessible PST files to improve computer performance requires MS Outlook to be open. While a technician has Outlook open, they may be exposed to the content of email messages, or see the senders or recipients of messages during this process. Such contact is incidental and is kept to the minimum required to successfully accomplish the task. Technicians are concerned with the wholesale movement of messages from one location to another to effect the requested repairs. It is impossible to separate access to PCI from incidental exposure of PCI during the course of specific operations. Technicians access *the minimum amount of PCI required* in order to successfully execute their task.

11) PCIO may be asked to extract and convey a particular file or files from a dataset to allow continued client operation while a computer system is being repaired. Testing the veracity of the subject file(s) is required prior to transmission. For example, the requested recovery of specific documents a client was working on, and needs to access, from a snapshot dataset while the computer is being repaired.

12) PCIO may be required to comply with a signed court order, which when properly executed relieves PCIO of any liability for releasing customer information to a third party. For example, in cases of divorce proceedings, criminal investigations, or civil proceedings.