Contractor Confidentiality Policy

It may be difficult to discern when to keep confidential certain information that is obtained through the course of working within the Root Capital ("Root") because the organization emphasizes the value of collaboration and sharing. In general, Root Capital contractors are expected to exercise utmost discretion regarding their work at Root Capital. Root Capital contractors should honor confidentiality obligations to Root and to all persons who share financial, personal, or sensitive information with Root contractors. Contractors are expected to NOT communicate any information they learn by reason of their positions that has not been made public, except as may be necessary in the course of their duties or upon authorization from a senior manager.

1. What kinds of information might be confidential?

Root Capital contractors may receive or see confidential, personal, or sensitive information about Root Capital, its employees, or its clients. Some examples of Confidential Information include:

- Compensation, health, and other personal data of employees or contractors
- Financial information of any party
- Credit card, social security, or financial account numbers (including bank identification numbers)
- Personal client information (*i.e.,* home address, phone number, work schedules, employment status, geolocation data, or financial information found in loan agreements and other documents)
- Root Capital's proprietary information such as business transaction details, trade secrets[1], and other intellectual property

2. Why does Root Capital need to protect confidentiality?

All of this "Confidential Information" should be protected for the following reasons:

a. The laws of a state or country may prohibit or limit sharing of certain information.

For example, the Massachusetts "Standards for the Protection of Private Information" law and federal privacy laws both require that personal information of an individual be protected. US federal law such as "HIPAA" (Health Insurance Portability and Accountability Act of 1996) aims to protect individually identifiable health information of all U.S. citizens. A limited number of Root Capital staff members who have access to such information are subject to keeping such health information strictly confidential.

Outside the United States, countries differ in how they approach data privacy and regulation. For example, the citizens of the European Union (EU) are protected by the EU Data Directive

[1] In general, a "trade secret" is any information that is economically valuable to Root Capital because it is not known by, or readily ascertainable by appropriate means to, others who could derive economic value from it. Trade secrets are protected from misappropriation under both state and federal law, but only as long as Root Capital makes reasonable efforts to keep them in confidence or maintain secrecy. The relevant information may include, but isn't limited to, formulas, patterns, compilations, methods, techniques, or processes.

("Directive") that imposes requirements on the processing and movement of personal data of EU citizens across EU member country borders. This means that if Root Capital contractors wish to move certain types of information about clients either into or out of an EU Country, the data must be handled and processed in compliance with the Directive. At a minimum, emails to and from an EU country must be encrypted or otherwise protected. Please consult with the designed Root point of contact in your contract (the "Point of Contact") for the contractor for safeguards to use in handling information or documents to or from persons in an EU country.

b. Root Capital contracts, other agreements, or understandings may require information or contract provisions to be kept confidential.

Non-disclosure agreements used by Root Capital with third party preclude these people from sharing Root's proprietary information, which may include trade secrets. However, anything outside of that defined list of items should first be cleared with the individual or organization providing the information. In general, legal contracts are confidential and should only be shared with those who need to see them in the course of their work.

c. Best practices may indicate the need to keep certain information confidential.

Even though Root Capital has no legal obligation in certain situations to keep information confidential, preserving confidentiality may be important for maintaining good client relations. For example, a client may view the names and details of one or more business contracts as confidential and may not want the information released to the public. Contractors should obtain client permission if there is any doubt about whether the client(s) would want the information shared with others.

d. Legal requirements and expectations of website users and donors inform our need to maintain the privacy of information provided online.

Root Capital posts its privacy policy on its public website (at the bottom of each page), and external websites such as Charity Navigator reference such policies for the public.

3. Where can confidential or personal information be found?

- Root Capital internal databases
- Contractor documents (agreements, applications, questionnaires, notes, client instructions such as wire transfer information)
- Files on the shared server, on laptops, in the cloud, or in paper form (especially pages printed or faxed which may be in the paper bins)
- Emails containing any of the items listed in #1 above or other confidential information
- Conversations about Root Capital proposed plans, overheard comments about clients

4. How can you protect confidential information?

It is clear that information should be protected when you see language that states "Confidential" or "Not for Public Distribution." Beyond that, be aware of what information might be confidential and think about whether it needs to remain private and protected. Check any policies or written agreements related to your contract on what information may be released

without further authorization and err on the side of caution. If you are not sure whether particular information should be treated as confidential, please contact your Point of Contact.

Take responsibility for protecting whatever confidential information you encounter. Get into the habit of checking your desk and printer bin to ensure that all sensitive information is either locked up or disposed of properly. If you handle checks, bank statements, or other documents that contain financial and personal information, ensure that they are not exposed to public view and are locked up when you are away from your desk. If the confidential information is in paper form and is no longer needed, destroy it promptly.

When you draft an email that contains confidential and/or personal information, decide whether you can send it securely by another method (such as fax or a telephone call) or if you can encrypt the information or the entire email. Emails sent within Root Capital's email system need not be encrypted separately since Root's emails are already encrypted. However, be aware that emails are often forwarded on to others, so it is a good habit to include "Confidential…" in the subject line of the email if applicable. You should notify the recipient that confidential information is enclosed and that it should be protected in compliance with this policy.

Do not store confidential or personal information of a third party on your computer in public/shared or personal drives and/or folders. This type of information should be accessible only to persons who have a need to see and use it. In addition, it is critical that no confidential information be stored on a computer (particularly a laptop) on its hard drive or desktop, or on devices such as CDs, thumb drives, or cell phones/PDAs. Root Capital's IT Team and its policies and procedures protect information while it is stored on the server or in the cloud, but any information stored locally is subject to loss or theft, particularly identity theft.

5. What is the potential harm if a confidentiality obligation is violated?

- Penalties under data security laws of the U.S., particular states, and/or global jurisdictions (such as the EU), including fines and lawsuits
- Potential lawsuits and penalties under any of the above laws for violation of privacy rights
- Damage to Root Capital's reputation and the confidence of clients, donors, lenders, and supporters

Preserving confidentiality of information is crucial for the maintenance of valuable relationships and the prevention of risk and liability to Root Capital. Please do your part to comply with the letter and the spirit of this policy.