

## CONFIDENTIALITY OF PROPRIETARY INFORMATION

It is the policy of CICF that its internal business affairs, confidential information, marketing strategies, donor lists and information, vendor lists, and methods of operation, are proprietary assets of the Foundation and that each employee will keep this information confidential.

1. Information designated as confidential (“Sensitive Data”) is to be discussed with no one outside the organization and only discussed within the organization on a "need to know" basis. In addition, employees have a responsibility to avoid unnecessary disclosure of non-confidential internal information about CICF, its donors, and its prospective donors. Decisions on confidentiality will be made by the President.
2. All employees are required to sign the Foundation’s “Nondisclosure and Confidential Information Agreement” (see the end of the manual). All employees must treat all aspects of their job and the information they learn as part of their job as proprietary property of CICF for which they are personally responsible.
3. Employees are specifically prohibited from attempting to obtain confidential information to which they are not entitled as a general and customary part of their job.
4. If an employee becomes aware of a data security breach in the course of their job they should notify management as soon as possible. Some events that may be considered security breaches include: Accidental disclosure of confidential data or Sensitive Data to outside parties, encountering a virus infection or spyware on a PC or server, loss of any computer hardware or storage device, and observing unauthorized access to software or a corporate website.
5. Employees that possess electronic door passes or other access devices (including keys) for access to CICF offices shall not give out or allow the access device to be used by anyone other than themselves. Access to facilities is restricted to employees and others where a business purpose exists. If an employee finds it necessary to have a person in CICF’s office or facility for any other reason, they must have prior management approval and appropriately monitor the guest.
6. Each supervisor, manager, executive, and director is responsible for the security of and control over information relating to CICF. Information identified as and designated as, confidential, will be clearly identified as such and properly secured.
7. All media inquiries and other inquiries of a general nature must be referred to the Director of Communications or to the President. All press releases, publications, speeches, or other official declarations must be approved in advance by the Director of Communications.
8. Employees who have direct personal or telephone contact with CICF donors are not to discuss with the officers, directors, or employees of other companies and foundations any confidential donor information.
9. Employees violating this policy will be subject to discipline, up to and including termination and may be subject to legal action.