Purpose: The intent of the following policy is to define how CDS will ensure that the confidentiality of its participants is not compromised by the use of Information Technology Resources. Security considerations for confidential information are described in more detail in policy P-1072 – Security.

Policy: It is the policy of CDS to utilize information technology resources in a manner that ensures the protection of the confidentiality of our participants. Federal and state laws, rules, regulations, policies, and procedures governing the confidentiality of data are not superseded, abridged, or amended by this policy.

Procedure and/or Process:

Limiting Access to Confidential Information:

- Access to Participant Information Systems (internal and external) is maintained by Data Systems personnel. All systems allow for several levels of access that control inquiry and/or update capabilities to what the person has a need to know. Each user has a unique user ID and password, and is granted a level of access commensurate to his/her responsibilities.
- When an employee leaves a workstation unattended, they must password protect the workstation (i.e. – lock their workstation within Windows). All CDS devices (desktop computers, laptops, cellphones, etc.) shall implement centrally-managed policies that set the device to automatically lock access after an appropriate amount of inactivity.
- Fax machines will be located in an area where an assigned person will ensure that faxes are kept confidential, and will promptly distribute them to the intended recipient. Fax machines will not be located in areas accessible to the general public.
- Any employee who intentionally obtains unauthorized access to confidential records shall be subject to discipline.
- Any employee who accidentally obtains unauthorized access to confidential records should inform his/her supervisor immediately.