Purpose: The intent of the following policy is to define how CDS will minimize risks associated with protection of Information Technology resources.

Policy: It is the policy of CDS to implement and enforce a level of security which will provide for the protection of data and information technology resources from accidental or intentional unauthorized disclosure, modification, or destruction by persons within or outside of the agency. Federal and state laws, rules, regulations, policies, and procedures governing the confidentiality of data are not superseded, abridged, or amended by this policy.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:

Security Officer:
- The Data Systems Manager (DSM) will operate as CDS's Security Officer.

Network Security:
- The agency-wide network is controlled by the Data Systems Department. Virtually every facet of daily activity requires this network to be functional and secure.
- Security of the network is the sole responsibility of CDS's Security Officer.
- CDS's entire network is placed behind hardware firewalls, and CDS's Security Officer will be alerted of intrusion attempts.
- Firewalls are set to use a central Syslog Server to archive access and changes.
- Connecting unauthorized equipment and personal electronics (cell phones, cameras, hard drives, flash drives, etc.) to CDS equipment and/or networks is forbidden. Violation of this may result in disciplinary action.
- All equipment must have the approved CDS standard anti-malware software installed and configured to automatically download current virus definitions. The Office 365 e-mail service is set to scan emails in real time and Windows Security automatically scans file downloads. Additionally, all Windows based computing equipment must have Microsoft Updates set to automatically download and install any critical updates. Violation of this may result in disciplinary action (refer to Policies P-1066 – Virus Protection; P-1067 – Hardware; and P-1068 – Software).

Critical Services Equipment:
- IT equipment for critical services will have reliability built into the equipment to ensure business continuity.
- IT equipment for critical services will utilize, when applicable, redundant technologies including RAID disk arrays to prevent one disk failure from interrupting services.
- IT equipment for critical services will utilize Uninterruptable Power Supplies that can provide power for a minimum of 15 minutes.
- Local critical services required for normal operation of the organization include:
  - Windows servers\Virtual Machine servers
  - MAS-90\Sage Accounting System
  - Phone systems (typically powered via network switches)
  - CCTV cameras and DVRs
  - Core network switches and hardware firewalls
  - Primary WAN routers & 4G failover WAN routers

Domain Access:
- Every CDS computer (both desktops and laptops) is to be joined to the CDSFL.org Windows AD/Azure AD domain.
- Every CDS employee issued a computer is to have an individual domain account.

- CDS employees that do not necessitate a dedicated computer are permitted to use a specific general-use computer as needed for training or other duties. Access is to be limited to an as-needed basis by their supervisor.
- Access is logged via Windows Event Logging, and forwarded to an event collection server.

Stand-alone Computers:

- Security measures for systems on stand-alone equipment will be the responsibility of the Information Technology Specialist.
- The use of a unique identifier for each individual user of stand-alone equipment will be required as identified by the Program Coordinator, and approved by the DSM.
- Prior to obtaining access to stand-alone equipment, personnel must have signed forms F-HR-1038 (HIPAA Training Acknowledgement Form) and F-HR-1039 Personnel Responsibilities in the Use of Information Technology Resources, as well as completed the on-line Privacy & Security Awareness Training course (within 2 weeks of employment for new hires).

Portable IT Devices:

This technology is easy to move from secure locations and therefore, poses a data security risk. These risks should be understood by each individual user. Below are CDS's minimum security requirements for use of this technology.

- If sensitive data is to be stored in removable media, including flash drives, the files must be password protected or the media must be protected by biometric lock, password, or encryption. If this information is written to and kept on this type of media, the media must be stored in a secure location when not in use.
- Confidential data should not be stored on any unencrypted mobile device (laptops, cellphones, flash drives, CDs, disks, etc).
- Staff may only use agency purchased, encrypted flash drives for sensitive data on agency owned hardware.
- If removable media devices are required, they must have encryption and they must be purchased and approved through the normal process.
- Removable media used in conjunction with agency business must also comply with disposal and data removal policies.
- Users of laptops are responsible for ensuring the adequate protection of not only the physical security of the laptop, but the data security for the information stored within the laptop.
  - All Laptops used for CDS work must be joined to the cdsfl.org domain in order to receive central management for security purposes.
  - No confidential information may be stored on an unencrypted laptop.
  - Laptops must always be physically secured when not in the personal possession of the assigned user.
  - Any thefts, losses or compromised security need to be immediately reported to the Program Coordinator, and the Security Officer who then must notify the COO and the CEO immediately. A report to Law Enforcement should be filed as appropriate.
  - Use of wireless technology shall utilize at a minimum 128 bit encryption.
- All staff will review and sign the Office of Inspector General Advisory on Inadequate Data Security on Mobile Devices.

Fax Machines:

- Faxes must be sent with CDS's authorized Fax Coversheets, which includes a confidentiality statement.
- When faxing HIPAA protected PHI, the sender must call the recipient before and after sending the fax to ensure someone is present to promptly receive and secure the information, unless the fax machine is known to be located in a secure location.
- Fax machines will be located in secure areas where assigned staff 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.

Participant Management Information Systems:

- All personnel who use equipment to access participant tracking systems resident at CDS Data Systems or access any agency or participant data by means of information technology resources owned by CDS will have unique personal identifier(s) and password(s). These should be kept confidential.
- Prior to obtaining a personal identifier(s) and password(s), personnel must have reviewed and signed forms F-HR-1038 (HIPAA Training Acknowledgement Form) and F-HR-1039 Personnel Responsibilities in the Use of Information Technology Resources, as well as completed the on-line Privacy & Security Awareness Training course (within 2 weeks of employment for new hires).
- Staff with access to contractually mandated databases will comply with all requirements as mandated by the specific contracts.
- The identifier(s) to contractually mandated databases will permit access to the data that the person has a need to know and will control inquiry and/or update capabilities. This access will be determined and authorized by the DSM. This initial security measure will ensure a general level of security across all systems.
- It is the responsibility of the employee to secure and protect their personal identifier. (i.e. – user ID and password)

Data Security:

- Backups of data critical to the operation of CDS will be maintained according to policy P-1065 – Backup.

Removal of Sensitive Data.

- Prior to the disposal of, off-agency repair, or "reuse" by another program, of an IT device, all sensitive data shall be removed and/or backed up from the IT device.
- Storage devices that will be disposed of must be disposed of in a fashion that meets HIPAA regulations to prevent its being read by any device that could potentially retrieve information from it.
- Any magnetic media that contains sensitive or confidential information that is being replaced due to repair/maintenance must be sanitized by approved methods. If these conditions cannot be met, then the media should be kept by CDS and disposed of in a fashion that meets HIPAA regulations.
- Only authorized Data Systems personnel should remove any sensitive data from IT devices. Documentation should be recorded on the Hardware Record form that shows when, how, and what method was used for sanitizing. Additionally, all surplus PCs and any removed disk drives or other small removable storage devices that have not yet been sanitized must have a label applied that indicates that the drive contains sensitive data.

E-mails:

- At no time shall confidential data be transmitted unencrypted via wireless devices or across unsecured public lines.
- Any e-mail containing confidential data sent via wired or wireless means must utilize at least 128-bit encryption and meet CDS software standards. Highly sensitive information should be placed into an MS Word document, password protected, then included as an attachment to the e-mail. The password used to lock the document should be given to the e-mail recipient over the telephone or sent in a follow-up e-mail. Alternatively, Microsoft OneDrive cloud storage may be used when paired with a password-protected link. (Refer to P-1008 – Electronic Transmission of Protected Health Information).
- Confidentiality Notice on E-mail. The following text is automatically included on all e-mail messages sent from computers:

> *IMPORTANT MESSAGE FOLLOWS: This message and its attachments are intended only for the individual to whom it is addressed. They are confidential and may contain legally privileged information. If you are neither the intended recipient nor the agent responsible for delivering the message to the intended recipient you are hereby notified that any dissemination of this communication is strictly prohibited and may be unlawful. If you feel you have received this communication in error please notify us immediately by return e-mail to the sender*

(and/or by telephone at 352.244.0628 ext.3753) and delete it from your system. We thank you in advance for your cooperation.

CDS Family & Behavioral Health Services, Inc.

Passwords:

- Passwords must be memorized, or if written down stored in a secured location.
- Staff must never use the "Remember Password" feature of applications, with the exception of CDS-authorized password management software (i.e. Bitwarden) that is also administered by Data Systems.
- Staff should use strong passwords of at least 8 characters in length, containing at least one capital letter and one number and/or symbol.
- Staff should not use the same password across multiple company systems.
- Staff must inform Data Systems personnel immediately, if they suspect their password has been compromised. This includes situations where staff believes they caught the possible breach before it was submitted or completed. Many attempts to steal credentials can often result in the partial or full capture of credentials, even when it appears the scam or phishing attempt was unsuccessful or incomplete.

Remote Access/Assistance

- Remote employees with a need to access local file shares or printers within the CDS network are provided VPN software and individual logins. Access is logged via the firewall handling the VPN connection, these logs are then forwarded to the central Syslog Server.
- All CDS workstations (both desktops and laptops) are to be pre-configured with a remote assistance client using ConnectWise ScreenConnect. The host platform's administration password is randomly generated and stored only within the BitWarden Password Manager. Sharing of the password between administration staff is to strictly take place only within the password manager.
- The remote assistance host platform is capable of allowing remote access to any PC with the client software installed. Administrative actions taken on the client PCs still require admin-level domain credentials.

Physical/Site Security:

- At a minimum, an annual analysis/review shall be conducted to determine the adequacy of physical/site security. It will take into account controlled physical access to the area, the need for disaster contingency planning, and other appropriate security requirements. The results of this review will be included in CDS's Risk Management Plan.
- The Risk Management Team will use preventive measures necessary to minimize the risk of destruction, theft and other losses of equipment, software, and data.
- The Risk Management Team will evaluate the physical location and conditions surrounding CDS sites and take the necessary precautions to protect them (e.g., locks may be required for each area where equipment is housed).
- End-users of IT resources should use prudent physical security to protect the equipment and data from destruction, theft, and other losses through limited physical and visual access. The aim is to physically protect the equipment and data from accidental disclosure, modification, or destruction. When an employee leaves a workstation unattended, they must password protect the workstation (i.e. – lock their workstation within Windows).

Personnel Orientation and Training:

- CDS's Security Officer will be responsible for providing policies, procedures, and guidelines on information security, which will be made available to and reviewed by all employees and volunteers during the orientation session and through the use of the computer based security awareness training course. This course must be completed within 2 weeks of hire.

- A Security Awareness Training program shall be maintained by the Human Resources Specialist that will ensure that employees are aware of the importance of information security. This program will provide annual security awareness training to all personnel that utilize confidential data or automated systems.
- All employees must complete Security Awareness Training before they are granted access to CDS applications.
- All CDS new employees will review applicable state and federal rules and regulations that pertain to data confidentiality and information security as a part of their orientation training.