# [ORGANIZATION]

# SUBJECT: Policy on Protecting Personally Identifiable Information

# EFFECTIVE: [DATE]

# APPROVED: [DATE]

1. **Protection of Client Information**

[ORGANIZATION] employees, agents, and subcontractors (hereafter known as “staff”) shall not disclose any individually identifiable client information to any person other than for the purposes of providing the requested services to the client and meeting its obligations under a contract agreement.

[ORGANIZATION] staff are permitted to disclose individually identifiable client information only with the consent of the individual for the purposes of meeting [ORGANIZATION]’s obligations under the any contract agreement.

# Training

[ORGANIZATION] shall instruct all staff with access to client information regarding the content of this document at least annually and for all new staff.

# Information Security Officer

[ORGANIZATION]’s Director of Finance and Operations is designated as the Information Security Officer to oversee [ORGANIZATION]’s compliance with this policy.

# Paper Document Controls

Supervision of Information. Client information in paper form shall not be left unattended at any time, unless it is locked in a file cabinet.

Escorting Visitors. Visitors to areas where the client information are contained shall be escorted and client information shall be kept out of sight while visitors are in the area.

Removal of Information. Client information must not be removed from the premises of [ORGANIZATION] except for identified routine business purposes or with express written permission of the client.

Mailing. Paper copies of client information shall be mailed using a secure, bonded mail service, such as Federal Express, UPS, or by registered U.S. Postal Service

Faxing. Client information that must be transmitted by fax shall require that staff confirms the recipient fax number before sending, and takes precautions to ensure that the fax was appropriately received.

# Technology Controls

Workstation/Laptop Encryption**.** All [ORGANIZATION]-owned or managed workstations, laptops, tablets, smart phones, and similar devices that process and/or store client information must be encrypted using algorithm which is 128 bit or higher. Any client information shall be encrypted at when stored on network file shares or document repositories.

Removable Media Devices**.** All electronic files that contain the client information must be encrypted when stored on any removable media or portable device (i.e. USB thumb drives, floppies, CD/DVD, smart phone, backup tapes etc.)

Only the minimum necessary amount of the client information required to perform necessary business functions may be copied, downloaded, or exported.

Antivirus Software**.** All [ORGANIZATION]-owned or managed workstations, laptops, tablets, smart phones, and similar devices that process and/or store client information must install and actively use comprehensive anti-virus software solution.

User IDs and Password Controls**.** All users must be issued a unique user name for accessing client information.

The system will maintain an automated audit trail which can identify the user or system process which initiates a request for client information, or which alters client information. The audit trail will be date and time stamped, log both successful and failed accesses, and restricted to authorized users.

Transmission Encryption**.** All data transmissions of client information by [ORGANIZATION] outside the secure internal network must be encrypted with a 128bit key or higher.

Encryption can be end to end at the network level, or the data files

# Requests for Client Information by Third Parties

[ORGANIZATION] staff shall promptly inform the Information Security Officer all requests for disclosure of any client information requested by third parties. The Information Security Officer, in consultation with Program Directors, shall determine an appropriate response.

[ORGANIZATION] shall maintain an accurate accounting of all requests for disclosure of client information.

# Destruction of Client Information

[ORGANIZATION] shall retain client documents only for as long as is required by contract agreement or local, state or federal law and in accordance with [ORGANIZATION]’s Document Retention policy. All client documents not required for retention will be promptly destroyed.

Confidential Destruction. Client information must be disposed of through confidential means, such as cross-cut shredding, or through certified third party vendors.

# Information Security Incidents and/or Breaches

Discovery and Notification of Information Security Incidents. Staff shall notify the Information Security Officer immediately upon the discovery of the information security Incident affecting the security of client information, or there is an intrusion, potential loss, actual loss, or unauthorized use or disclosure of the client information.

The Information Security Officer shall document all corrective actions taken to mitigate the risks or damages involved with the Information Security Incident and/or Breach and to protect the operating environment.

Isolation of System or Device**.** A system or device containing client information compromised by an exploitation of a technical vulnerability shall be promptly disconnected or quarantined and investigated until the vulnerability is resolved.

Investigation of Information Security Incidents. [ORGANIZATION] shall promptly investigate information security incidents and produce a written report of the investigation, to include but not be limited to the following:

* Description of what happened, including the date of the incident and the date of the discovery of the incident and/or Breach, if known;
* Description of the types of client information that were involved and the extent of the information involved;
* A description of the unauthorized persons known or reasonably believed to have improperly used or disclosed client information;
* A description of where the client information is believed to have been improperly transmitted, sent, or utilized;
* A description of the probable causes of the improper use or disclosure;
* Full, detailed corrective action plan, including information on measures that were taken to halt and/or contain the information security incident.

# Protection of Confidential Information of Employees, Agents, and Subcontractors

[ORGANIZATION] employees with access records of [ORGANIZATION] employees, agents, and subcontractors shall not disclose any confidential information pertaining to [ORGANIZATION] other than for the administration of human resources and contractual and volunteer agreements. The same precautions in protecting client information shall be followed in protecting confidential staff information.

While all individually identifiable client information is considered to be confidential, staff information that is confidential includes but is not limited to:

* Personal information, including home address, personal phone number, social security number, immigration status, and marital status
* Employment and salary history
* Employment benefits received and information to establish benefits eligibility
* Performance reviews and disciplinary actions

Only the following employees shall have access to confidential staff information:

* [ORGANIZATION] Executive Director
* Director of Finance and Operations
* Administration Manager with responsibility in human resources

Employee Signature Date