

## ***State of Massachusetts - Outline of Standard Operating Procedures (SOPs) Manual<sup>1</sup>***

### **SECTION 1: Contractual Requirements and Roles**

CSPTech Contract Requirements: CSPTech, in its role as the central server, agrees to provide all of the necessary equipment and staff to operate and maintain the central site. This includes all required licenses for software and direct technical assistance to sites. This applies to all programs and agencies that CSPTech is currently funded to serve.

CSPTech New Sites Requirements: Any agency that CSPTech does not receive alternate funding for but does want to participate must assume the costs of requisite licenses and cost-share of central resources.

Steering Committee: CSPTech utilizes the steering committee to provide general oversight and guidance to the project. The committee is composed of representatives of each group of stakeholders. This includes consumers, agency directors, frontline staff, and state agencies that provide service to the homeless population.

Central Server Management: Management of an HMIS requires several divergent skill sets. The CSPTech project has identified the following roles to provide the best, most efficient service to our stakeholders:

- ◆ Database Administrator;
- ◆ Applications Administrator/Technical Assistant;
- ◆ Network Assistant;
- ◆ Report Writer/SQL Programmer; and
- ◆ Technical Assistant.

The project also designates the roles of every participating user in order to prevent any confusion around responsibilities and privileges. Each role must be filled in order for the agency to begin working with the project:

- ◆ Role: Participating Agency Executive Director;
- ◆ Role: Participating Agency Site Technical Administrator; and
- ◆ Role: User.

---

<sup>1</sup> For more detail on standard operating procedures see the forthcoming *Implementation Guide: Homeless Management Information Systems*, Center for Social Policy, McCormack Institute of Public Affairs, University of Massachusetts Boston prepared under subcontract with Aspen Systems Corporation in partnership with the U.S. Department of Housing and Urban Development, 2002.

## ***State of Massachusetts - Outline of Standard Operating Procedures (SOPs) Manual'***

### **SECTION 2: Participation Requirements**

Participation Requirements: For most efficient utilization of the services provided by CSPTech, several steps must be completed at the agency level before implementation can begin. Central server staff assists with most steps though some require the agency to act without assistance. Steps include:

- ◆ High Speed Internet Connectivity (DSL or Broadband);
- ◆ Identification of a Site Technical Administrator to serve as primary contact;
- ◆ Completed security assessment and signed contract; and
- ◆ Establishing client consent procedures and interview protocols.

Central Server Requirements: This section covers the exact equipment, staffing, and procedures that the CSPTech staff is responsible for. Focused on security, the areas are:

- ◆ Hardware Physical Security;
- ◆ Software Security;
- ◆ Network security;
- ◆ Over-the-wire security; and
- ◆ Client database security.

Implementation Requirements: Agencies must generate documents that cover each of the following areas in order for implementation to begin.

- ◆ Interagency Data Sharing Agreements: Agencies that will be sharing client specific records must agree in writing to uphold the same standards of privacy protection.
- ◆ Written Client Consent Procedure for Electronic Data Sharing: Agencies that will be sharing client specific records must have documented releases of information from each client.
- ◆ Confidentiality and Informed Consent: For agencies that do not share client specific records CSPTech requires the development of a verbal explanation regarding the project to give to each client entering the program.
- ◆ Interview Protocol: Each agency must develop a program specific interview guide that includes the minimal data elements and any additional elements the agency wishes to collect.
- ◆ Data Collection Commitment: Participation in the CSPTech project requires that all participating programs collect minimum data elements on all consenting clients.
- ◆ Information Security Protocols: Internal policies must be developed at each site to establish a process for the violation of any of CSPTech's information security protocols.
- ◆ Implementation – Connectivity: Once implementation has begun each site agrees to maintain connectivity in order to continue project participation.
- ◆ Maintenance of Onsite Computer Equipment: Each agency agrees to maintain computer equipment in order to continue project participation.

## ***State of Massachusetts - Outline of Standard Operating Procedures (SOPs) Manual'***

- ◆ Conversion of Legacy Data: Agencies that are using legacy systems that request data conversion must provide resources and processes to enable conversion unless specific contracts have been established to provide the conversion at no cost.

### **SECTION 3: Training**

Training Schedule: CSPTech provides ongoing training on all relevant aspects of system operation for the duration of the project. Training modules are developed based on skill level and type of access to the system. Each user of the system is required to complete basic user training in order to begin using the system.

User, Administrator and Security Training: Depending on the role a staff person has they must attend specific training to fulfill that role. Each training contains an information security component.

Scheduled Training Delivery: CSPTech agrees to deliver at least monthly group trainings on a regional basis.

Onsite Training: CSPTech is available to deliver on-site training in the event that an agency has a large number of staff to train. CSPTech will not deliver one to one training on-site.

### **SECTION 4: User, Location, Physical and Data Access**

Access Privileges to System Software: Access to system resources will only be granted to agency staff that need access in order to perform their job.

Access Levels for System Users: Each user of the system will be assigned an account that grants access to specific system resources that they require. A model of least-privilege is used; no user will be granted more than the least amount of privilege needed to perform their job.

Location Access Privileges to System Server: CSPTech requires that each computer accessing the system be identified and authorized prior to access. CSPTech uses electronic certificates in order to accomplish this goal.

Access to Data: All data collected by the CSPTech project is categorized. Access to datasets, types of data, and all CSPTech data releases is governed by policies developed by the Steering Committee.

Access to Client Paper Records: All users of the system must not have greater access to client information through the system than is accessible in the agencies paper files.

## ***State of Massachusetts - Outline of Standard Operating Procedures (SOPs) Manual'***

Physical Access Control: All equipment or media containing CSPTech data must be physically controlled at the central site. Protections and destruction policies vary depending on the type of data and media.

Logical Access: Access to system resources must be limited to authorized users for authorized transactions.

Unique User ID and Password: Each user of the system must be individually and uniquely identified. Identification will be verified through a password.

Right to Deny User and Participating Agencies' Access: CSPTech retains the right to suspend or revoke the access of any agency or individual to the system for consistent or egregious violation of CSPTech policies.

Data Access Control: Access to the system must be audited. All audits must be reviewed regularly.

Auditing – Monitoring, Violations and Exceptions: CSPTech considers any exception to stated security policies a violation of those policies that must be investigated.

Auditing – Data Logs: CSPTech will maintain logs of all actions taken by central server staff. Logs include SQL2000 logs, Windows logs, and firewall logs. All logs are reviewed regularly.

Data Assessment and Access: All data associated with the CSPTech project is categorized. Access to data is restricted based on the content of the data. Reproduction, distribution, and destruction of data is based on the content of the data.

Data Integrity Controls: Access to the production data is restricted to essential central server staff only. Each staff that has access to production data is contracted to not alter or impact data in any way.

Local Data Storage: If agencies choose to store local copies of data they are encouraged to developed policies and procedures on how data is generated, stored, and destroyed.

Transmission of Client Level Data: All participating agencies and the central server staff agree to transmit any client level data securely.

Electronic Transmission of Authenticators: Authenticators are any mechanisms used to identify users or computers. CSPTech staff agree to not transmit authenticators electronically.

### **SECTION 5: Technical Support and System Availability**

Planned Technical Support: CSPTech offers a standard technical support package to all participating agencies. Support services include training, implementation support, report writing support, and process troubleshooting.

## ***State of Massachusetts - Outline of Standard Operating Procedures (SOPs) Manual'***

Participating Agency Service Request: Service requests from participating agencies must originate from either the executive director or site technical administrator. Central server staff are not permitted to respond to requests from other site staff.

Rapid Response Technical Support: Requests for service that require a rapid response will be responded to within 1 business day.

Availability – Hours of System Operation: The system is available to users 20 hours a day. The system is scheduled for two 2 hour time blocks of potential downtime.

Availability – Central Staff Availability: Central server staff are available during normal business hours to respond to service requests.

Availability – Planned Interruption to Service: Participating agencies will be notified of planned interruptions to service one week prior to the interruption.

Availability –Unplanned Interruption to Service: In the event of an unplanned interruption to service central server staff will make a determination if the cause can be repaired within 2 hours. If the determination is that the primary system cannot be repaired within 2 hours the secondary system will be brought into production.

### **SECTION 6: Stages of Implementation**

Implementation – Stage 1. Start-up and Initial Training: Implementation begins with stage 1. To enter stage 1 an agency must complete all requisite paperwork and create user accounts on the system.

Implementation – Stage 2. Data Entry Begins: To enter stage 2 an agency must begin entering data on their client population. To move to stage 3 an agency must be entering information on at least 25% of their clients or entering information for 2 continuous months.

Implementation – Stage 3. Basic Information on Most Clients: Stage 3 lasts for 6 months. Agencies must move out of stage 3 within six months. In order to move out of stage 3 an agency must be entering basic information on at least 60% of their client population.

Implementation – Stage 4. System Fully Integrated in Daily Operation: Stage 4 is the final stage of implementation. To classify as stage 4 an agency must be entering information on 100% of their client population or be continuously entering information for at least 12 continuous months.

## ***State of Massachusetts - Outline of Standard Operating Procedures (SOPs) Manual'***

### **SECTION 7: Encryption Management**

Encryption General: All potentially identifying information is encrypted in the database. Encryption prevents unauthorized personnel from accessing confidential information for any reason.

Encryption Management: In the event that system wide data decryption becomes necessary the process is outlined here. Only one event has been identified that would require this, a change in products. To execute this decryption CSPTech must obtain the written authorization of every participation agency's executive director.

### **SECTION 8: Data Release Protocols**

Data Release Authorization and Distribution: CSPTech does release data in the process of generating reports. CSPTech agrees to only release contextual data that covers at least 60% of geographically defined population. CSPTech will only release de-identified aggregate data.

Right to Deny Access to Client Identified Information: CSPTech does not release client identified information to any third party. Court orders for information will be forwarded to the University of Massachusetts Institutional Review Board for review. Pursuant to IRB policy no release will occur unless the party obtains the written release of every client within the database prior to receiving the database.

Right to Deny Access to Aggregate Information: CSPTech retains the right to deny access to aggregate level data. Pursuant to Steering Committee policy any interested party must file a Request for Data. All requests are reviewed by central server staff and the Steering Committee.

### **SECTION 9: Internal Operating Procedures**

CSPTech maintains policies and procedure that address several internal functions of a web based HMIS. Unfortunately the release of internal policies and procedures would impact the functionality of the system. Therefore internal procedures are not available.

Communities interested in web based HMIS should address each of the following areas:

- ◆ Computer Virus: Prevention
- ◆ Computer Virus: Detection of Virus Infection
- ◆ Computer Virus: Disinfection
- ◆ Electronic Internal Communication: Use of Email, Attachments and Distribution Lists
- ◆ Backup and Recovery: Preventive Measures
- ◆ Backup and Recovery: Backup
- ◆ Backup and Recovery: Archiving
- ◆ Backup and Recovery: Disaster Recovery
- ◆ Disaster Recovery Process