Life Recovery Services

Technology Plan

Annual Review of Procedures for Business Continuity/Disaster Recovery

1/4/2022

Information Technology Department Description and Policies: The Executive Director is identified as the lead person for issues relating to the information management system throughout the agency. IT services are contracted with Tom Milberg, under the direction and supervision of the agency's Executive Director. He is responsible for day-to-day operations, administration, application, infrastructure support, and maintaining compliance with all applicable laws, rules, and accreditation standards.

Information Confidentiality: Life Recovery Services maintains confidential, protected health information regarding its clients, some of which is maintained electronically. This agency also maintains proprietary business information that must be protected from unauthorized and/or unlawful access. All electronic documents or files containing confidential treatment or administrative information that are created, maintained, modified, updated, or copied using an agency computer and/or server must be stored in a location that is secure from unauthorized access and/or encrypted.

Confidential information is defined as:

1. Electronic Protected Health Information (EPHI): Electronic health information or health care payment information, including demographic information collected from an individual, which identifies the individual or can be used to identify the individual. Individually identifiable information refers to any coding or descriptive information by which there is a reasonable basis to believe that the information can be used to identify the individual or by which the individual has been identified in the past. This includes but is not limited to the following:
    a. A person's name (including initials),
    b. Customer number,
    c. Address (including zip code),
    d. Nickname by which the person may be called or commonly known,
    e. Physical description,
    f. Description of a particular physical and/or behavioral characteristic, condition, or diagnosis;
2. Any medical and/or behavioral health information that may be maintained by the company regarding any of its employees or contract workers is considered EPHI;
3. Proprietary Business Information (PBI): Information contained in any of the following:
    a. Employee records,
    b. Contract information and files,
    c. Company form data,
    d. Financial data,
    e. Strategic planning information,
    f. Company policies and procedures.

Any electronic transmission of confidential information must be protected against unauthorized or unlawful access during the transmission process. This may be accomplished by the encryption at the security level specified within the HIPAA standards and/or utilization of a standardized electronic transfer format specified within the HIPAA standards.

Confidential Electronic Information may not be removed from company property on portable computers or any removable media. Removable media is defined as any of the following:

a. Any media or device that is not internal to the company PC that can store electronic files and information that can be connected to or inserted into another computer that will allow access to the data stored on that device.
b. This includes but is not limited to CD-R/RW and DVD to any of the following:
    1. Externally attached hard drives,
    2. CD-R/RW media,
    3. Flash memory devices,
    4. Unmanaged smart phone.

All employees and contract workers are granted clearance to view and edit confidential electronic information based upon their job functions within the following matrix:

Job Function	View Confidential Admin. Info.	Edit Confidential Admin. Info.	Transmit Confidential Admin. Info.	View Confidential Treatment Info.	Edit Confidential Treatment Info.	Transmit Confidential Treatment Info.
IT Contractor	**X**	**X**	**X**	**P**	**P**	**P**
Executive Director	**X**	**X**	**X**	**X**	**X**	**X**
Leadership Team	**X**	**X**	**X**	**X**	**P**	**P**
Clinical Staff	**N**	**N**	**N**	**X**	**X**	**N**
Medical Staff	**N**	**N**	**N**	**X**	**X**	**P**

Matrix Key: **X** = Clearance Granted; **P** = Clearance Granted by Executive Director's Approval; **N** = No Clearance Granted

Life Recovery Services' staff/contract workers may not transmit or otherwise remove confidential information from an agency computer and/or server unless:

1. It is within the scope of their job function to do so,
2. The staff/contract worker has the appropriate clearance level to do so,
3. Authorization to do so has been granted by the responsible program director.

Storage: Confidential electronic information that must be saved by employees is to be stored by all users with registered MS Office 365 accounts in One Drive. Documents and files are to be stored in a user's "My Documents" folder on Windows based workstations, which is automatically backed up to the corporate iDrive account. These folders may only be accessible from password protected User accounts and a secure browser. Employees may not store confidential electronic information in their personal computers' local hard drives or non-encrypted local drives. Contract workers may store confidential electronic information in their personal or business computers only after the execution of a contract which delineates the scope of work which will be performed.

Staff will be trained to place all workstation documents on the server instead of the individual workstations. This is to secure any data in the event of theft, fire, etc. All documents that are saved to the server will then be backed up via normal operations.

System Security: All access to electronic records maintained by the agency is restricted by use of strong passwords. All use of IT resources on the local area network (LAN) and iDrive is secured by use of strong passwords. IT resources include, but are not limited to the following:

1. Company owned computers, Smart Phones, and all data and files stored on them,
2. Company owned Removable Devices and hard drives and all data and files stored on them,
3. Networked public or private folders on the company servers and all data and files stored on them and/or Cloud Drives (iDrive, Google Drive, etc.),
4. All email and contact information on the Google Exchange Server and/or transmitted across company Network Infrastructure,
5. All Internet usage via company Network Infrastructure,

All company owned computers, whether they are logging into Windows Server domain accounts or local workstation accounts are secured from unauthorized access in the following manner:

1. Computers from which it is possible to access confidential client or business information are located within a secure location, with at least one locking door between the computer's location and public areas of the facility. The only exception to this rule is the computer at the reception desk.
2. Computers from which it is possible to access confidential client or business information are configured with the requirement of a strong password upon startup of the PC and upon exiting the screen saver on a running PC.

3. Remote access to company IT resources shall be granted only to registered Domain Users on the discretion of the Executive Director. All access will be protected by strong passwords and VPN Technology or secure SSL via remote desktop connection.
4. Windows based workstations and servers are protected by AVG Antivirus, HitmanPro Crypto, and/or Windows Defender. Definition updates and regular scanning are centrally managed and performed regularly. Managed Microsoft Patching is also implemented, and updates/rollouts of critical patches and updates will occur regularly.
5. Managed Network Firewall is in place with 24X7 Monitoring with HIPAA/PCI Compliant cloud management service.
6. In December 2021, a Security Risk Assessment/Procedure for Business Continuity/Disaster Recovery Evaluation was completed and Life Recovery Services has implemented the findings and recommendations from this report. We also plan to complete them annually to keep our organization up to date with changing technology and security requirements and HIPAA regulations and Meaningful Use compliance.

While Life Recovery Services seeks to provide a reasonable level of privacy, all persons utilizing the system/accessing records on the system must be aware that all data or files created or stored on the Life Recovery Services system are the intellectual property of Life Recovery Services. The single exception to this standard is any electronic information concerning clients and their treatment, which is adjunct to their medical record and, therefore, the property of the client him/herself. Electronic information concerning clients and their treatment belongs to the client, however Life Recovery Services maintains custody of this information and, therefore, the security standards included in this policy and procedure are in full effect.

Failure to adhere to this policy and procedure, inappropriate use of company IT resources, and/or actions that place the security of Life Recovery Services IT resources and/or electronic records may result in the following:

1. Revocation of access privileges,
2. Possible disciplinary/contract action up to and including termination of employment/contract.

Inappropriate use of company IT resources include the following:

1. Access and/or viewing of client records without a need to know for business, payment, or treatment purposes.
2. Access and/or viewing for personal gain.
3. Access and/or viewing for reasons that are counter to the best interests of Life Recovery Services and/or its clients.

Upon separation of employment/termination of contract with Life Recovery Services, the IT Department personnel must be notified immediately to ensure that the individual's access to IT resources is immediately disabled. The IT Department must be notified regardless of the reason for the employee's/contract worker's separation from Life Recovery Services. If access to IT resources is not immediately disabled, access to IT resources by a former employee/contractor is unlawful and subject to legal action.

System Backup: All Life Recovery Services servers are automatically backed up every night. Backups include the following:

1. System volume information,
2. System state data,
3. Application data,
4. The content of all user folders.

Backups are stored on a local backup secure server. Key users' workstations are also backed up incremental nightly and full backups nightly using the iDrive Cloud Service.

Disaster Recovery: It is the responsibility of the Information Services Department to implement and maintain the following measures to protect against catastrophic loss of data:

1. There are 2 redundant local backups,
2. There is 1 nightly full backup stored in the cloud

Use of Assistive Technology: Assistive technology products are designed to provide additional accessibility to individuals who have physical or cognitive difficulties, impairments, and disabilities. When selecting assistive technology products, it is crucial to find products that are compatible with the computer operating system and programs on the computer being used.

Below are descriptions of the various types of assistive technology products that are currently available on the market today.

Alternative input devices allow individuals to control their computers through means other than a standard keyboard or pointing device. Examples include the following:

1. Alternative keyboards—featuring larger- or smaller-than-standard keys or keyboards, alternative key configurations, and keyboards for use with one hand.
2. Electronic pointing devices—used to control the cursor on the screen without use of hands. Devices used include ultrasound, infrared beams, eye movements, nerve signals, or brain waves.
3. Sip-and-puff systems—activated by inhaling or exhaling.
4. Wands and sticks—worn on the head, held in the mouth or strapped to the chin and used to press keys on the keyboard.
5. Joysticks — manipulated by hand, feet, chin, etc. and used to control the cursor on screen.
6. Touch screens — allow direct selection or activation of the computer by touching the screen, making it easier to select an option directly rather than through a mouse movement or keyboard. Touch screens are either built into the computer monitor or can be added onto a computer monitor.

Braille embossers transfer computer generated text into embossed Braille output. Braille translation programs convert text scanned programs in or generated via standard word processing into Braille, which can be printed on the embosser.

Keyboard filters are typing aids such as word prediction utilities and add on spelling checkers that reduce the required number of keystrokes. Keyboard filters enable users to quickly access the letters they need and to avoid inadvertently selecting keys they don’t want.

Light signaler alerts the computer user with light signals. This is useful when a computer user cannot hear computer sounds or is not directly in front of the computer screen. As an example, a light can flash alerting the user when a new message has arrived, or a computer command has completed.

Onscreen keyboards provide an image of a standard or modified keyboard on the computer screen that allows the user to select keys with a mouse, touch screen, trackball, joystick, switch, or electronic pointing device. Onscreen keyboards often have a scanning option that highlights individual keys that can be selected by the user. Onscreen keyboards are helpful for individuals who are not able to use a standard keyboard due to dexterity or mobility difficulties.

Reading tools and learning disabilities programs include software and hardware designed to make text based materials more accessible for people who have difficulty with reading. Options can include scanning, reformatting, navigating, or speaking text out loud. These programs are helpful for those who have difficulty seeing or manipulating conventional print materials; people who are developing new literacy skills or who are learning English as a foreign language; and people who comprehend better when they hear and see text highlighted simultaneously.

Screen enlargers/magnifiers work like a magnifying glass for the computer by enlarging a portion of the screen which can increase legibility and make it easier to see items on the computer. Some screen enlargers allow a person to zoom in and out on a particular area of the screen. Screen readers are used to verbalize, or "speak," everything on the screen including text, graphics, control buttons, and menus into a computerized voice that is spoken aloud. In essence, a screen reader transforms a graphic user interface (GUI) into an audio interface.

Screen readers are used to verbalize, or "speak," everything on the screen including text, graphics, control buttons, and menus into a computerized voice that is spoken aloud. In essence, a screen reader transforms a graphic user interface (GUI) into an audio interface. Screen readers are essential for computer users who are blind.

Speech recognition or voice recognition programs allow people to give commands and enter data using their voices rather than a mouse or keyboard. Voice recognition systems use a microphone attached to the computer, which can be used to create text documents such as letters or by voice.

This agency remains committed to providing services to clients and guests with disabilities, as well as staff with special needs. Life Recovery Services will remain current on what is available and the feasibility of utilizing this technology with our clients.

Summary of Current Technology and Spending: When the agency was started, we only had 2 Desktop Computers. We have expanded to one computer in each office, the reception area, and the pharmacy. We currently have 2 database servers and 1 backup server. We are currently in a five-year PC refresh cycle replacing most desktop computers. It remains sensible for Life Recovery Services to spend very conservatively on its Information Technology needs. However, as growth continues, it has become imperative that we focus our attention on several areas listed below that will be critical toward achieving and sustaining our Strategic Plan and growth.

1. Computer Hardware: All existing hardware will be assessed and upgraded as necessary. Equipment has been purchased within the last 3 years. We estimate that equipment will need to be replaced every 5 years.
2. Software and Licensing: All work stations have been assessed and necessary software will be installed. This agency will purchase End User License Agreements for all software utilized. Base Server, HitmanPro Crypto, Windows Defender, and AVG antivirus for small business have been installed.
3. Network Infrastructure: LAN with high-speed internet connection with a new modem, one primary network printer, and supporting equipment have been implemented and upgrades are scheduled this year to optimize network speed and access. New wireless access points and upgrades will be implemented and improved.
4. Disaster Recovery: Experience has revealed that the most common threat we face daily is the loss of our connectivity to the Internet. When we lose access to the Internet and to LEO, e-mail, etc., this leaves us “dead in the water” and severely impacts our ability to function. This results in a very unfavorable situation for our staff and our clients. We have implemented an LAN connection through the router for our workstations to the server regardless of internet connectivity.

Electronic Medical Record Implementation: an EHR from Tohubohu Clinical Solutions was implemented the first quarter of 2019. We train staff to use the software and review as needed. We are also continuously adding enhancement requests and preparing new forms to use this year. This is an ongoing project which requires quarterly review with the leadership team and feedback from staff. Authorization for services and billing are currently being completed in by hand via the secure Oklahoma Health Care Authority website.

COVID-19: This past year has challenged our organization with the Covid-19 pandemic, lockdown, and guidelines provided by the Governor, ODMHSAS, and OHCA. We were tasked with creating a much more mobile workforce and method to provide Tele-health services to our clients as a primary service. While we were in a good position from the first day of these new directives, we had many challenges we had to overcome. We were able to implement secure video services which allow us to schedule and conduct large scale Zoom meetings for both individual and group sessions. We were tasked with purchasing more webcams to allow the new software to run. We have now offered remote desktop connections to staff to ensure their ability to access the server from remote locations. We upgraded all of the desktop computers within the office to accommodate the new standards of care during the pandemic and continue to move in this direction. All our solutions are safe, secure, and meet the requirements for HIPAA privacy, ODMHSAS, and CARF standards. We will continue to take feedback from clients, staff, and stakeholders in an effort to improve upon the hardware, software, and processes to provide the best possible services possible.

Priorities: The software updates have been completed. However, we acknowledge that we need to update the hardware as quickly as possible. We will plan to upgrade/replace 1 workstation every 6 months. In order to accomplish this, the agency must reallocate funds.

Technology Maintenance: Refer to the IT contract for software and hardware updates/maintenance.

Technology Acquisition: This agency defers the acquisition of new software and hardware to the contracted IT department. Before any new items are purchased, a proposal must be submitted to and approved by the Executive Director.

Annual Review of Procedures for Business Continuity/Disaster Recovery:
In December 2021, a Security Risk Assessment/Procedure for Business Continuity/Disaster Recovery Evaluation was completed by Tom Milberg. Life Recovery Services has implemented the findings and recommendations from this report. We also plan to complete them annually to keep our organization up to date with changing technology and security requirements and HIPAA regulations and Meaningful Use compliance.

- Effectiveness:
    - An attempt to restore data was conducted. All service restoration points in time were working correctly.
- Areas Needing Improvement:
    - Shadow copies need to be changed from 1 time to 2 times each day.
    - Some passwords from staff members were found to be weak to moderate strength and exceeded the 3 month policy for change requirements.
- Actions Needing Improvement:
    - IT department needs to check shadow copies on a weekly basis to ensure no data loss.
    - Frequency for password resets need to be established and set at no more than 3 months.
- Actions to Address the Improvements Needed:
    - IT department changed the frequency of shadow copies from 1 time to 2 times each day.
    - IT department changed the frequency of password resets to no more than 3 months.
    - Changes implemented the requirements of a “strong” password as well.
- Implementation of the Actions:
    - Configuration was set at 6 hour intervals during business hours to ensure that we have no longer than 6 hours of data loss.
    - Staff members were required to change secure passwords at this time using a requirement for “strong” passwords.
- Whether the Actions Taken Accomplished the Intended Results:
    - The actions showed that the configurations were successful.
- Necessary Education and Training of Personnel:
    - IT Department educated the Executive Director as to where the scheduling configuration is located in the system.
    - IT Department educated the Executive Director as to how to restore a shadow copy backup in the event of his unavailability.
    - IT Department educated the staff about what constitutes a “strong” password.
    - IT Department will schedule a staff training in March to implement procedures of the remote desktop connections with user names and passwords and the configuration of it on their personal computers.

IT Support Contract

Introduction

This IT support contract describes the services that Life Recovery Services (‘the client’) will receive from Thomas Milberg (‘the supplier’).

Purpose

The client depends on IT equipment, software and services (together: ‘the IT system’) that are maintained and supported by the supplier.

This IT support contract sets out how the IT supplier will provide maintenance and support services for the IT system. It describes for which items the supplier will provide support, what activities it will perform, and how the client can expect problems with the IT system to be handled.

Scope

Parties

This IT support contract is between:

The client:	The supplier:
Life Recovery Services 5113 SE. 15th Street Del City, OK. 73115 Key contact: Cody Shoemaker 580 304 9770 cody@okliferecovery.org	Thomas Milberg 3806 N. Ann Arbor #5 Oklahoma City OK. 73122 Key contact: Tom Milberg 405 686 8788 milbergtom@gmail.com

Dates and reviews

This contract begins on **01/01/2020** and will run for a period of **[36] months.**

It may be reviewed at any point, by mutual agreement. At the end of the contract, the supplier and client will discuss possible renewal terms.

Equipment, software, and services covered

This contract covers the equipment, software and services listed in the table below. This list may be updated at any time, with agreement from both the client and supplier.

Exclusions

As this IT support contract is written in a spirit of partnership, the supplier will always make the best-possible efforts to provide support and rectify problems as requested.

However, this agreement only applies to the parts of the IT system listed above.

Additionally:

- This contract does not cover IT system problems caused by using equipment, software or service(s) in a way that is **not recommended**.
- If the client has made **unauthorised changes** to the configuration or set up of equipment, software or services, this agreement may not apply.
- If the client has prevented the supplier from **performing required maintenance and updates**, there may be a delay in resolving issues.

This contract does not apply to circumstances that could be reasonably said to be beyond the supplier's control. For instance: floods, war, acts of god and so on.

This contract also does not apply if the client fails to pay agreed supplier invoices on time.

Having said all that, [supplier] aims to be helpful and accommodating at all times, and will do its absolute best to assist [client] wherever possible.

Responsibilities

Key supplier responsibilities

The supplier will maintain and support the IT system used by the client.

Additionally, the supplier will:

- Ensure relevant software, services and equipment are available to the client in line with the service level agreement (SLA) that accompanies this contract.
- Respond to support requests as described in the SLA — and within reasonable time, in any case.
- Do its best to escalate and resolve issues in an appropriate, timely manner.
- Maintain good communication with the client at all times.

Key client responsibilities

The client will use the IT system covered by this contract as intended.

Additionally, the client will:

- Notify the supplier of issues or problems in a timely manner.
- Provide the supplier with access to equipment, software and services for the purposes of maintenance, updates and fault prevention.

- Keep the supplier informed about potential changes to its IT system. For example, if staff are to begin connecting their own mobile devices to the company network, the supplier may be able to adjust its services accordingly.
- Maintain good communication with the supplier at all times.

Activities

The supplier will perform a number of specific activities for the client. Details of these activities are described in the table below, along with the purpose and frequency of each.

Activity	Frequency	Notes
General		
Document software and hardware changes	As necessary	
Send client log of work performed	Monthly	
System Maintenance		
Check backups are running properly	Daily	This is a simple check that backups are running with no errors reported.
Perform backup test	Monthly	This is a full data restore test.
Monitor and maintain server uptime	Constantly	
Install software patches, service packs and other updates	As necessary	Updates will usually be tested before being rolled out across the IT system.
Install software upgrades	As necessary	Upgrades that incur costs — and other major upgrades — will only be installed after consultation with the client.
Monitor server event logs for potential problems	Daily	
Monitor status and availability of cloud services	Constantly	Automated systems will be used to check cloud services used by the client are available.
Monitor available disk space on servers and company computers	Daily	
Perform system and server reboots	As necessary	Non-essential reboots will be performed at convenient times, agreed between client and supplier.
General server maintenance	As necessary	To be performed out of hours or at mutually agreed times.
Let client know of any potential issues	As necessary	For example: • Disk space running low • Equipment showing signs of failure • Deteriorating broadband speed
Create, remove and maintain employee user accounts and permissions	As necessary	For example, when employees: • Join or leave the company • Require access to additional resources
Assist users with support queries	As necessary	For example: • How to connect to VPN • Where to save shared files •

Fixing Problems		
Disaster recovery of core systems	As necessary	In the event of a significant IT failure or problem (e.g. complete server failure or security breach), the supplier will do everything possible to restore service. A separate disaster recovery plan should be maintained.
Fix user errors / mistakes	Help Desk	For example: • Accidental file deletion • Forgotten password
Raise support requests with third-party providers	As necessary	Where cloud services and other aspects of the IT system are not in the supplier's direct control, the supplier will take responsibility for liaising with third-parties to resolve issues.
Managing Networks		
Maintain internet connection	Constantly	Automated monitoring will be used to identify performance issues with or availability of the client's internet connection(s).
Monitor router logs	Weekly	
Monitor network capacity and performance	Weekly	The supplier will endeavour to identify where network capacity is reaching its limit.
Maintaining Security		
Monitor firewall logs	Monthly	The supplier will attempt to identify and address any unusual or suspicious activity.
Check status of security software updates	As necessary	The supplier will verify that all updates are installed in a timely manner.
Investigate any suspicious activity or unexpected software behaviour	As necessary	The supplier will investigate any activity that could be the result of malicious software or individuals, such as viruses or hacking attempts.
Manage file and folder permissions	As necessary	
Enforce password policies	As necessary	
Confidentiality		
The Supplier may have access to and receive "Confidential Information" (defined in the next section) about its staff, volunteers, mission, clients who it serves, and donors whose contributions are critical to the organization's ability to serve its clients. Service Provider understands and shall ensure that each of its employees and agents or contractors understands that Client owns its Confidential Information, it is a key asset of Client, and Client has the right to protect its Confidential Information from being given to or disclosed to any person or entity outside the organization without written authorization, of Client on behalf of the Service Provider and each of its employees and agents or contractors who shall be bound by this Agreement. Service Provider enters into this Agreement voluntarily.		

Definition of Confidential Information

In this Agreement, “Confidential Information” consists of all and each of the following:

1. Client Materials. This part of the definition extends to non-public Client documents, notes, files, records, oral information, computer files and similar materials, and all copies of same, about all and each of the following: The organization’s mission and activities; strategic plans; financial information; business policies, procedures, and techniques; or development projects or results; trade secrets; clients lists, client health information, and information maintained about Client donors, prospective clients, donors, and prospective donors; and any information about Client.
Service Providers and other business partners.

2. Confidential Information of Third Parties. This part of the definition extends to information that relates to or is claimed by a client, prospective client, donor, or prospective donor to be such person’s confidential information. Service Provider, shall respect and keep such information strictly confidential, and not disclose such information to any person or organization, without the written authorization of Client.

Service Provider’s Promises

1. Unless authorized in writing by Client, Service Provider will keep all Confidential Information and will not copy, reproduce, or make notes of, divulge to anyone or any entity outside Client, or use any of the Confidential Information for Service Provider’s or another’s benefit or purpose. This includes during the period of time Service Provider is rendering services to Client, and after Service Provider’s contract ends.

2. Both during the period Service Provider is performing services for Client, and after Service Provider’s contract with Client, terminates, Service Provider will, when asked, promptly surrender and deliver to Client, (and will not keep in Service Provider’s possession or deliver to anyone else or other entity) the Confidential Information and all copies of same, and any and all other property of Client.

Remedies

1. Service Provider understands that a violation of this Agreement likely will result in disciplinary action including possibly the termination of Service Provider’s contract with Client. Service Provider further understand that Client will have the right to go to court to obtain any equitable and legal remedies that are appropriate for Client to protect its legal rights in its Confidential Information. Service Provider agrees that Oklahoma law governs this Agreements and its interpretation

2. Client waiver or failure to enforce any violation or provision of this Agreement will not constitute a waiver of its rights hereunder with respect to any violation or provision of this Agreement, and will be effective only if in writing, signed by Client, and then only in the specific instance and for the specific purpose given.

This IT support contract is agreed between Life Recovery Services and Thomas Milberg

Signed on behalf of the client:	**Signed on behalf of the supplier:**
Name: Life Recovery Services	Name: Thomas Milberg
Position: Executive Director	Position: Owner/Operator
Date: 01/01/2020	Date: 01/01/2020
Cody Shoemaker MSC NCGC-II LADC/MH	Thomas Milberg