LIFE RECOVERY
SERVICES, INC.

TECHNOLOGY PLAN

ANNUAL REVIEW OF PROCEDURES FOR BUSINESS CONTINUITY / DISASTER RECOVERY

1/13/2023

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 2022, 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 2022, 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.