Easy ET Technology Solutions PLC

Information security and confidentiality Policy

January 01 2022

PURPOSE:

To protect the confidentiality and privacy rights of individuals served by First Call For Help of Easy Et, and other service providers with whom the agency cooperates, to establish standards of client and administrative record confidentiality, to guide the conduct of employees and volunteers (all hereinafter referred to as "Users") of Easy Et in their handling of client and agency information and to inform its employees of their obligation to protect the infrastructure and information assets.

The following list of authoritative citations apply; more information can be found in the Office of Early Learning (OEL) Grant award.

• 2 CFR 200.335, Methods for collection, transmission and storage of information

• OEL IT Security Manual

• OEL Program Guidance 101.02, Records Confidentiality

• Computer-related Crimes, Chapter 815, F.S.

SCOPE:

IT Security is the responsibility of every Information Systems User (volunteers, employees, Managers, Directors and Administration). The policy applies to all Easy Et employees, contractors, temporaries and consultants who use the agency systems. As such, all Department Information Systems Users must be informed of the information technology security policies. It is the policy of Easy Et that:

• Information resources are valuable assets of Easy Et and, as such, must be protected to some degree from unauthorized disclosure, modification, or destruction, whether accidental or intentional.

• Electronic protected health information shall be protected following the Health Insurance Portability

and Accountability Act of 1996 (HIPAA) Policy as outlined herein.

• The privacy of student education records shall be protected following the Family Educational Rights and Privacy Act (FERPA) (20 U.S.C. § 1232g; 34 CFR Part 99).

• In the event a disaster or catastrophe disables information processing functions, the ability to continue critical Easy Et Engineering PLC services must be assured.

• Security controls required by law must be complied with and standards, where applicable, must be met or exceeded. The expense of security enhancements beyond the minimum requirements must be appropriate to the value of the assets being protected.

• Security awareness and training is one of the most effective means of reducing vulnerability to errors and fraud and must be continually emphasized and reinforced.

• Violation of the Confidentiality and Information Security Policy shall subject the individual to discipline appropriate to the infraction, up to and including immediate termination.

OBJECTIVES:

The objectives of this policy are to establish agency wide Information Technology (IT) Security Policies that:

• Prevent the misuse, denial and loss of information assets

• Establish responsibility and custodial roles for the protection of information

• Prevent statutory or regulatory violations

• Preserve Easy Et management options in the event of loss or misuse of public and private information.

• Clarify Information Systems (IS) User responsibilities and duties regarding protection of information resources.

• Enable Managers, Directors and IS User to make good decisions about information security.

Achievement of these objectives will ensure the confidentiality, integrity and availability of the information entrusted to us.

Policies are grouped into three categories:

1. Administrative
2. Technical
3. Program

KEY CONCEPTS:

Breach of Security: The unauthorized access of data containing personal information. Good faith access of personal information by an employee or agent of the company does not constitute a breach of security, provided that the information is not used for a purpose unrelated to the contract or subject to further unauthorized use.

Confidential: Refers to entire record systems, specific records or individually identifiable data that by law are not subject to public disclosure. When applicable, confidentiality covers all documents, papers, computer files, letters and all other notations of records or data that are designed by law as confidential. Further, the term confidential also covers the verbal conveyance of data or information that is confidential. These confidential records may include but not be limited to, social security numbers, parent and child information, payments, childcare providers, household demographics and resource and referrals, which are private and confidential and may not be disclosed to others.

Information Technology Security: The protection of an automated information system to preserve the integrity, availability, and confidentiality of data, information, and information and technology resources.

Personally Identifiable Information (PII): PII means information that can be used to distinguish or trace an individual's identity, either alone or when combined with other personal or identifying information that is linked or linkable to a specific individual. Some information that is considered to be PII is available in public sources such as telephone books, Web sites, and university listings. This type of information is considered Public PII and includes for example, first and last name, address, work telephone number, and general educational credentials.

The definition of PII is not anchored to any single category of information of technology. Rather, it requires a case-by-case assessment of the specific risk that an individual can be identified. Non-PII can become PII whenever additional information is made publicly available, in any medium and from any source, that, when combined with other available information, could be used to identify an individual.

Security Incident: The attempted or successful unauthorized access, use, disclosure, modification, or destruction of information or interference with Easy Et operations; random attempts at access shall not be considered a security incident.

ADMINISTRATIVE POLICIES:

The following policies are administrative in nature and pertain to DOs and DON'Ts. Proper use of IT

resources and other network services are covered. These policies are in direct support of Security Administration processes.

INFORMATION SECURITY AWARENESS STANDARDS:

The Information Security Awareness Standards will ensure that all IS Users are informed and aware of the importance of protecting the sensitive information held by the Department prior to being granted access (via a User Confidentiality Security Agreement attached) to any Easy Et System. This will also ensure that IS Users are aware of information security threats and concerns, and are equipped to support Easy Et's IT security policies in the course of their normal work. The Information Security Awareness Standards establishes the requirement for security awareness and education of all IS Users that access to Easy Et's information systems and assets. Information assets include any valuable or sensitive information in any form created, gathered or stored and used as a component of a business process.

1. IS Users will be informed of security procedures and the correct use of information processing facilities to minimize possible security risks. This includes security requirements, legal responsibilities and business controls, as well as training in the correct use of information processing facilities e.g. log-on procedures, use of applications, if applicable, before access to information or services is granted. The following steps must be followed:

• Our company shall ensure that IS Users are aware of the Easy Et's current IT security policies.

• Easy Et shall inform new full-time and part-time users, employees, temporary workers, contractors, vendors and consultants (IS Users) of the importance of information security and their role in protecting valuable and sensitive information systems and assets during their orientation.

• IS Users shall acknowledge in writing that they have been informed and are aware of the policies.

IT SECURITY INCIDENT HANDLING STANDARDS:

These standards describe the procedure for managing computer security incidents and provide Easy Et Users with information on what to do if they discover a security incident. Another purpose is to minimize the damage from security incidents and malfunctions, and to monitor and learn from such incidents.

The term incident in this policy is defined as any irregular or adverse event that occurs on any part of the Easy Et's Information Systems. Some examples of possible incident categories include: compromise of system integrity; denial of system resources; illegal access to a system (either a penetration or an intrusion); unauthorized access to confidential data; malicious use of system resources, or any kind of damage to a system.

The steps involved in handling a security incident are categorized into five stages:

• Protection of the system

• Identification of the problem

• Containment of the problem

• Eradication of the problem

• Recovering from the incident and the follow-up analysis

Appropriate steps will be taken against any user who violates the terms of this policy.

1. IS Users shall note and report any observed or suspected security weaknesses in, or threats to, systems or services. They should report these matters either to their immediate supervisors or Director who in turn should report to the Department Data Services Director.

2. IS Users should not attempt to prove a suspected weakness as testing weaknesses might be interpreted as a misuse of the system.

3. A computer security incident can occur at any time of the day or night. Thus, time and distance considerations in responding to the incident are very important. IT security incidents are classified into three levels depending on severity:

• Level 1 incidents are the most serious and should be handled immediately or as soon as possible. Level 1 incidents must be escalated to the Department Information Systems Manager or designee.

• Level 2 incidents are less serious but should still be handled the same day that the event occurs (usually within two to four hours of the event). Level 2 incidents should be escalated to the Department Information Systems Manager or designee.

• Level 3 incidents are the least severe, but it is recommended that they be handled within one working day after the event occurs. Level 3 incidents should be escalated to the Department Information Systems Manager or designee.

4. Reporting an incident:

Logging of information is critical in situations that may eventually involve federal authorities and the possibility of a criminal trial. The implications from each security incident are not always known at the beginning of, or even during, the course of an incident. Therefore, a separate written log shall be kept by each member of the incident handling team for all security incidents that are under investigation.

The incident report should record all necessary factual details including:

• The nature of the unauthorized use or disclosure

• The confidential information used or disclosed

• Who made the unauthorized use or received unauthorized disclosure

• What happened

• How, where and when the incident occurred

• What Easy Et had done or shall do to mitigate any deleterious effect of the unauthorized use of disclosure; and

• What corrective action Easy Et has taken or shall take to prevent future unauthorized use or disclosure.

Easy Et is subject to the reporting timeframes of critical incidents below:

Report as soon as possible and no longer than 30 minutes of the incident to a Security Officer, Manager, or Program Officer (for extenuating circumstances to President/CEO as needed). The written notification shall be made within 24 hours after Easy Et learns of the security incident or breach. Easy Et is also required to report to OEL/ELC in writing within 24 hours after the Easy Et learns of the security incident or breach and this portion of the process/instructions is not included in policy for staff. Easy Et and any of its employees, agents, contractors, affiliates or any other individual who breach security or confidentiality are subject to any state or federal criminal sanctions and civil remedies provided by law.

5. Each log entry shall contain the date and time of the action being documented by that log entry. The information in the log must not be altered, so the log must be securely stored in a location with restricted access so that it cannot be altered by others. Manually written logs are preferable since on-line logs can be altered or deleted. Entries made in the log shall be handwritten in blue or black ink.

6. Upon successful completion of the incident handling, all logs shall be forwarded to the Contractor local administrator who will ensure that the original is copied for maintaining in the Contractor's files before forwarding the original to the Department Information Systems Manager or designee. The types of information that shall be logged are:

• Dates and times of incident-related phone calls

• Dates and times when incident-related events were discovered or occurred

• Amount of time spent working on incident-related tasks

• Actions taken by Easy Et

• People Easy Et contacted

• Names of systems, programs or networks that have been affected

7. Although virus and worm incidents are very different, the procedures for handling each are very similar aside from the initial isolation of the system and the time criticality. Worms and some viruses are self-replicating and can spread to hundreds of machines in a matter of minutes, thus, time is a critical factor when dealing with a worm attack.

• Isolate infected system(s) from the remaining network as soon as possible. Network isolation is one method to stop the spread of a worm, but the isolation can also hinder the clean-up effort since Easy Et will be disconnected from sites which may have patches. The Department Information Systems Manager or designee must authorize the isolation of the network from the outside world. Log all actions. Do not power off or reboot systems that may be infected. There are some viruses that will destroy disk data if the system is power-cycled or re-booted. Also, re-booting a system could destroy needed information or evidence.

• Notify Appropriate People as outlined above.

• Try to identify and isolate the suspected virus or worm-related files and processes. Prior to removing any files or killing any processes, a snapshot of the system must be taken and saved.

<u>Below is a list of tasks to make a snapshot of the system:</u>

o Save a copy of all system log files.

o Save a copy of the root history file.

o Capture all process status information into a file.

If specific files that contain virus or worm code can be identified, then move those files to a safe place or archive them to tape and then remove the infected files. Also, get a listing of all active network connections

• Contain the virus or worm. All suspicious processes shall now be halted and removed from the system. Make a full dump of the system and store in a safe place. The tapes should be carefully labeled so they will not be used by unsuspecting people in the future. Then remove all suspected infected files or worm code. In the case of a worm attack, it may be necessary to keep the system(s) isolated from the outside world until all systems have been inoculated and/or the other Internet sites have been cleaned up and inoculated. Log all actions.

• Inoculate the System(s). Implement fixes and/or patches to inoculate the system(s) against further attack. Prior to implementing any fixes, it may be necessary to assess the level of damage to the system.

If the virus or worm code has been analyzed, then the task of assessing the damage is not very difficult. However, if the offending code has not been analyzed, then it may be necessary to restore the system from backup tapes. Once the system is brought back into a safe mode, then any patches or fixes shall be implemented and thoroughly tested. Log all actions.

• Return to a Normal Operating Mode. Prior to bringing the systems back into full operation mode, Contractor should notify the same group of people who were notified in stage one. The users should also be notified that the systems are returning to a fully operational state. The Department Information Systems Manager or designee will determine if it is necessary for all users to change their passwords and notify them as needed. Before restoring connectivity to the outside world, verify that all affected parties have successfully eradicated the problem and inoculated their systems. Log all actions.

• Follow-up. After the investigation, a short report describing the incident and actions that were taken must be completed. Log all actions.

IT SECURITY RISKS STANDARDS:

These standards places the accountability and responsibility of performing IT security risk assessment on Easy Et administrators. The purpose of the risk assessment is to determine areas of vulnerability, and to initiate appropriate remediation.

1. An initial IT security risk assessment must be performed on every critical business application/system by the Easy Et IT Department.

2. Users are expected to cooperate fully with any Risk Assessment being conducted on systems for which they are held accountable.

3. Users are further expected to work with the Risk Assessment Team in the development of a remediation plan.

INFORMATION TECHNOLOGY STANDARDS:

The purpose of these standards is to outline the acceptable use of Easy Et Systems assets and resources. These standards are intended to protect Easy Et from risks including virus attacks, compromise of network systems and services, and legal issues. This standards applies to Contractor's which contract with Easy Et, its users and pertains to all IT assets and resources owned or leased by the Easy Et.

1. Access to Department IT assets and resources is a privilege. It requires individual users to act responsibly, conserve computer resources, and consider the rights and privacy of others. The assets and resources (i.e. (laptops, computers, monitors, mice, keyboards, PDAs, printers, telephones, fax machines,

etc.) are the property of Easy Et.

2. Easy Et has the right, but not the duty, to monitor any and all aspects of its information system, including, but not limited to, monitoring employees use of the internet, reviewing material downloaded or uploaded by employees, and reviewing e-mail sent and received by employees. Employees waive any right to privacy in anything they create, store, send, or receive on the 2-1-1's information systems.

3. Users should be aware that they may be subject to the laws of other states and countries when they engage in electronic communications with persons in those states or countries or on other systems or networks. Users are responsible for ascertaining, understanding, and complying with the laws, rules, policies, contracts, and licenses applicable to their particular uses.

4. The following uses of Department IT resources are prohibited:

A. Interference or impairment to the activities of others, including but not limited to the following:

1. Authorizing another person to use Department computer systems. Contractors are responsible for all of their accounts. Contractors must take all reasonable precautions, including password maintenance and file protection measures, to prevent use of their account by unauthorized persons. Users and employees of Contractors must not share their password with anyone else or provide access to the Department network resources to unauthorized persons.

2. Unauthorized access and use of the resources of others, including but not limited to the following:

a. Use of Department resources to gain unauthorized access to resources of any other individual, institutions, or organizations.

b. Use of false or misleading information for the purpose of obtaining access to unauthorized resources.

B. Accessing, altering, copying, moving, or removing information, proprietary software or other files (including programs, libraries, data and electronic mail) from any network system or files of other users without proper authorization.

C. Damage or impairment of Department resources, including but not limited to the use of any resource irresponsibly or in a manner that adversely affects the work of others, such as:

1. Hacking – attempting to obtain or use passwords, IP addresses or other network codes that have not been assigned to you or authorized for use as Contractor employees, attempting to obtain unauthorized access to computer accounts, software, files, or any other Department IT resources.\

2. Malicious Activity – intentionally, recklessly or negligently damaging any system (e.g., by the introduction of any so-called "virus", "worm", or "Trojan-horse" program); damaging or violating the

privacy of information not belonging to the user; or misusing or allowing misuse of system resources.
3. Any other activity not specifically cited above that may be illegal, harmful, destructive, damaging, or inappropriate use of Department IT resources.
D. Unauthorized commercial activities, including but not limited to the following:
1. Using Department resources for one's own commercial gain, or for other commercial purposes not officially approved by the Department, including web ads.
2. Using Department resources to operate or support a non-Department related business.
E. Violation of local, state or federal laws, including but not limited to, violating any laws or participating in the commission or furtherance of any crime or other unlawful or improper purpose.
Easy Et reserves the right to monitor computer and network usage for operational needs and to ensure compliance with applicable laws and Easy Et policies.

AUDIT POLICY STANDARDS:

This standard provides the authority for members of the IS Department to conduct security audits and covers any system or equipment on or connected to Easy Et Systems. Audits may be conducted to:
A. Ensure integrity, confidentiality, and availability of information and resources
B. Investigate possible security incidents to ensure conformance to Department security policies
C. Monitor user or system activity where appropriate.
1. When requested and for the purpose of performing an audit, any access needed for the audit will be provided to members of the IS Department.
This access may include:
A. User level and/or system level access to any computing or communications device
B. Access to information (electronic, hardcopy, etc.) that may be produced, transmitted, or stored on equipment or premises
C. Access to work areas (labs, offices, cubicles, storage areas, etc.)
D. Access to interactively monitor and log traffic on the Easy Et Systems.

SECURITY ADMINISTRATION STANDARDS

These standards covers all computer and communication devices on the administrative network owned or operated by the Easy Et. The security of a computer system involves safeguards for the hardware, software, and the data stored in the system. Computer system security also involves the protection of stored data and the prevention of unauthorized access and alteration of stored data. Each individual has

responsibilities related to maintaining security over the Easy Et information assets. Security administration should be involved in developing security policies where they do not exist and reviewing policies for effectiveness where they do exist. The function must be involved in the enforcement of security standards and in setting sanctions for noncompliance with established policies, procedures, and standards.

Department IT Security Administration

1. The Data Services Director is the IT Security Point of Contact who is responsible for controlling and monitoring physical and electronic access to Easy Et specific information assets.
2. Must ensure the ongoing protection of Easy Et specific information assets by establishing proper and adequate logical access controls, including password security and other access restrictions, to ensure that only authorized personnel have access to the automated systems within Easy Et.
3. Ensure that all Users adhere to the security policies, guidelines and procedures.
4. Ensure that we have the software to monitor the adequacy of system hardware, performance and capacity-related issues has been implemented.
5. Monitor the adequacy of system hardware, performance and capacity-related issues has been implemented.
6. Coordinate the process to manage employee accounts, including processing request for new accounts, establishing accounts and closing accounts as well as tracking accounts and employee access authorizations.
7. Provide staff specific access privileges on each system, limited to those required to perform their job functions.
8. Monitor and provide audit trails, i.e., system log-ins, log-outs, deleted files, have been implemented.
9. Periodically review user privileges and modify, revoke, or deactivate, as appropriate
10. Create and enforce security policies.
11. Ensure that password security functions, features, and capabilities are activated for Easy Et systems.
12. Ensure that passwords are of sufficient length and complexity that they cannot be easily compromised.
13. Ensure that passwords are changed for all online users. Users with more sensitive capabilities (e.g., security administrators, certain users of financial and payroll systems) may want to change their passwords more frequently.

14. Establish adequate password security on automated systems.

15. Review terminal logs and security violation reports.

16. Monitor activity on remote access facilities to ensure that only authorized personnel are using them.

17. Detect and monitor access to systems or information outside the normal patterns or needs of a user or specific workstation.

18. Maintain security over Department information to ensure that unauthorized access does not occur.

19. Report potential security breaches to Contractor Management. Monitor and track repeated security violators.

20. Maintain historical records of security violations for at least 90 days.

21. Provide suggestions and recommendations to Easy Et on security-related matters.

22. Research and suggest, as requested, additional security devices, such as modems with dial-back capability, which can potentially improve security.

23. Closely monitor the following:

A. Individuals with access to any tool that can change programs or data, such as program compilers, data-altering utilities, report generators, and text editors.

B. Documentation for managing access criteria for information resources.

C. Audit trails to provide accountability for all accesses to confidential and exempt information and software.

D. Audit trails for all changes to automated security or access. Examples include removal of access privileges, computer accounts and authentication tokens.

E. Remote access lines, especially those with dial-up and VPN capabilities.

F. Terminated employees, especially those with high-tech capabilities.

G. Procedures for unfriendly termination(s) that include prompt removal of system access.

H. Unfriendly terminations have prompt removal of system access.

I. Removal of access privileges and computer accounts.

J. Return any office information resources (property, data).

K. Return of any Coalition information resources (property or data).

L. Repeat violators who claim not to understand log-on procedures.

All IS End-users

1. Adhere to all established security policies.

2. Required to understand and comply with the Florida Computer Crimes Act, Chapter 815, Florida Statutes. The minimum security requirements are: passwords are not to be disclosed and information is not to be obtained for the individual or another person's personal use.

3. Report suspicious systems activity, which may indicate that files or programs have been tampered with to the Contractor's IT Security Point of Contact, agency management, and to the Department.

4. Refrain from sharing confidential user codes, passwords, or other codes intended to restrict access to information assets.

PHYSICAL SECURITY STANDARDS

The Physical Security Standards clearly establishes steps that must be considered to ensure access to computer facilities and information assets are adequately protected. This includes, but is not limited to:

A. Physical security perimeter

B. Physical entry controls

C. Security of data centers and computer rooms

D. Securing individual personal computer and laptops

E. Securing employee desks and open areas.

1. Physical security perimeters. Physical security protection should be based on defined perimeters and achieved through a series of strategically located barriers throughout the location. The requirements and placement of each security barrier should depend upon the value of the assets and information to be protected, as well as the associated risk. Each level of physical protection should have a defined security perimeter around which a consistent level of security protection is maintained. The following guidelines for physical security perimeters are provided:

A. Security of the perimeter should be consistent with the value of the assets or services under protection.

B. Security perimeter should be clearly defined.

C. Support functions and equipment (e.g., photocopiers and fax machines) should be located to minimize the risks of unauthorized access to secure areas and exempt information.

D. Physical barriers should, if necessary, be extended from floor to ceiling to prevent unauthorized entry and environmental contamination.

E. Other personnel should not be made aware unnecessarily of the activities within a secure area.

F. Prohibition of individuals working alone should be considered, both for safety and to prevent opportunities for malicious activities.

G. Organizationally managed computer equipment should be housed in dedicated areas separate from third- party managed computer equipment.

H. When vacated, secure areas should be physically locked and periodically checked.

I. Support services personnel should be granted access to secure areas only when required and authorized; where appropriate, their access should be restricted (especially to exempt information) and their activities monitored.

J. Photography, recording or video equipment should not be allowed within the security perimeters, unless authorized.

2. Physical entry controls. Easy Et safeguards confidential information resources (i.e., network servers, backups and other databases, etc.) by limiting physical access to these areas of the administrative office by non-authorized individuals. Secure areas should be protected by appropriate entry controls to ensure that only authorized personnel are allowed access. Unauthorized individuals will be escorted by personnel with authorization. The following controls should be considered:

A. Visitors to secure areas should be supervised (entry and departure).

B. Visitors should only be granted access for specific, authorized purposes.

C. All personnel within the secure area are encouraged to challenge strangers.

D. Access rights to secure areas should be revoked immediately for personnel that terminate employment.

3. Any keys or other access devices issued to the employee must be returned as part of the termination process.

4. Security of data centers & computer rooms. Data Centers and computer rooms supporting critical organizational activities should have stringent physical security. The selection and design of the site should take account of the possibility of damage from fire, flooding, explosions, civil unrest and other forms of natural or manmade disaster. Consideration should also be given to any security threats presented by organizations and/or businesses in close proximity. The following measures should be considered:

A. Where possible, buildings should be unobtrusive and give minimum indication of their purpose, with no obvious signs, outside or inside the building, identifying the presence of computing activities.

B. Lobby directories and internal telephone books should not identify locations of computer facilities.

C. Backup equipment and media should be situated at a safe distance to avoid damage from a disaster at

the main site.

D. Appropriate safety equipment should be installed, such as heat and smoke detectors, fire alarms, fire extinguishing equipment and fire escapes; fire suppression and safety equipment should be checked regularly in accordance with manufacturers' instructions; employees should be properly trained in the use of safety equipment.

E. Emergency procedures should be fully documented and regularly tested.

F. Doors and windows should be locked when unattended, and external protection should be considered for windows.

5. Employee desk/open area policy. To reduce the risks of unauthorized access, loss, and damage to information after normal working hours, exempt and restricted papers and diskettes should not be left on desks unlocked. Information left out on desks is also likely to be damaged or destroyed in a disaster. The following guidelines should be applied where appropriate.

A. Papers and diskettes should be stored in cabinets when not in use, especially outside of working hours.

B. Exempt or critical organizational information should be locked away (ideally in a fire-resistant cabinet) when not required, especially when the office is vacated.

C. Key locks, passwords, or other controls should protect personal computers and computer terminals when not in use.

D. Consideration should be given to the need to protect incoming and outgoing mail points and unattended fax machines.

IT SECURITY PROGRAM STANDARDS

The purpose of these standards is to establish, implement and continuously improve the IT Security Program. This program must be sufficient enough to guarantee the integrity, accuracy and availability of information for which Easy Et's has custodial responsibility. The program must reduce the risk of unauthorized disclosure, modification or destruction of information to a level. User, Managers and Directors will be held accountable.

1. The DS Director, or designee, will place a monetary value on all data, software and information system resources owned by Easy Et for risk management purposes.

2. The DS Director, or designee, will identify which information resources are sensitive and take steps to protect such information from disclosure or unauthorized modification.

3. The DS Director, or designee, will identify which information resources are essential to the continued

operation of critical Easy Et functions and take steps to ensure their availability.

4. The DS Director, or designee, will evaluate IT Security enhancements beyond the minimum requirements for their cost effectiveness and to apply those which can be cost justified considering the exposure.

TECHNICAL POLICIES

The following policies are technical in nature and must be implemented by all Easy Et Users. Access to information and resources available through the Easy Et's network systems must be strictly controlled to prevent unauthorized access. Access to all computing and information systems and peripherals shall be restricted unless explicitly authorized.

TECHNICAL STANDARDS

1. Access to operating system commands is to be restricted to those persons who are authorized to perform systems administration/management functions.

2. The network security policies are intended to protect the integrity of the Easy Et's Systems and to mitigate the risks and losses associated with security threats to the system.

3. The following policies should be read and cross referenced as part of the Easy Et's Network Security.

A. Privacy Practices Act – HIPAA Policies

4. In support of this policy, the IT Department will:

A. Monitor in real-time, network traffic as necessary and appropriate for the detection of unauthorized activity and intrusion attempts, and

B. Publish security alerts, vulnerability notices and patches and other pertinent information.

ANTI-VIRUS STANDARDS

A computer virus is an unauthorized program that replicates itself and spreads onto various data storage media and/or across a network. The symptoms of virus infection include considerably slower computer response time, inexplicable loss of files, changed modification dates for files, increased file sizes, and total failure of computers. Because viruses have become very complex, users must not attempt to eradicate them from their systems. If users suspect infection by a computer virus, they must immediately stop using the involved computer and call the IT Department.

1. The IS department must ensure that all departmentally-managed computers have virus protection that is in keeping with the standards set out in the security policy.

2. The IS Department is responsible for maintaining and updating this Anti-Virus Policy.

3. The IS Department will keep the anti-virus products it provides up-to-date in terms of both virus definitions and software version in use. This will be done online via the normal and periodic updates of the Anti-virus definition files.
4. Where necessary and appropriate the IS Department will apply any updates to the anti-virus services it provides that are required to defend against threats from viruses and other malware threats.
5. The IS Department will install anti-virus software on all owned, leased and installed desktop workstations, laptops, portable devices and servers. Note: Every server or computer that contains OEL data or conducts any form of OEL business runs antivirus software.
6. The Antivirus software must protect data, scan documents, attachments, emails and Internet sites before use. In addition to the Antivirus program must scan portable media devices (e.g., flash drives, CDs, storage devises) before use.
7. The IS Department must maintain documentation to verify the purchase, installation and use of antivirus software.
8. The IS Department will assist employees in installing and/or updating anti-virus software according to standards on personally-owned computers that will be used for business purposes. The IS Department may, at its discretion, provide anti-virus software in these cases if it is deems critical to the preservation of the security integrity of the network.
9. Virus checking programs approved by the IS Department are continuously enabled on all servers and networked personal computers (PCs) as well as on Easy Et laptops issued to staff.
10. The IS Department will take appropriate action to contain, remove, and assist in recovery from virus infections. In order to do so, the IS Department may be required to disconnect a suspect computer from the network or disconnect an entire segment of the network.
11. The IS Department will perform regular anti-virus sweeps of the entire network.
12. Where Users are allowed to use personally-owned or mobile computers for business purposes an adherence to the virus protection processes and procedures that are in keeping with the standards set out in this policy will be enforced.
13. Users are responsible for taking reasonable measures to protect against virus infection.
14. Users must not attempt to either alter or disable anti-virus software installed on any computer attached to the internal network of Easy Et without the express consent of the IS Department.

PASSWORD STANDARDS

The Password Standards outlines the handling, responsibilities, and scope of passwords for Easy Et's Systems.

1. Passwords shall be controlled to prevent their disclosure to unauthorized persons. Users and Easy Et shall control their passwords to prevent their disclosure to unauthorized persons.

2. Passwords for all systems are subject to the following rules:

Password Creation Protocol

A. All passwords must have at least (8) characters, and should consist of a mixture of letters, numbers and special characters.

B. User passwords should contain at least one alphabetic and one non-alphabetic character. Non-alphabetic characters include numbers (0-9) and punctuation. Acceptable Characters are: A – Z, a-z, 0-9, and!@#$ %&*() _-+=.

C. Passwords cannot be reused for at least six (6) changes.

D. Never assign a login account a password that is the same string as the Employee ID or that contains the Employee ID (e.g., "bob123" is not an appropriate password for employee "bob").

E. Never set any password equal to the null string (i.e., a blank password), which is equivalent to no password at all.

F. Passwords should not contain any proper noun or the name of any person, pet, child, or fictional character.

G. Passwords will not contain any associate serial number, Social Security Number, birth date, telephone number, or any information that could be readily guessed about the creator of the password.

H. Passwords should not contain any simple pattern of letters or numbers, such as "xyz123."

I. Passwords should not share more than three (3) sequential characters in common with a previous password (i.e., do not simply increment the number on the same password, such as fido1, fido2, etc.).

J. Use a password that is easy to remember (e.g., a phrase, line from a song, or nonsense words) and that you can type quickly. Password Storage and Visibility.

Password Storage and Visibility

A. Passwords will not be visible on a screen, hardcopy or other output device.

B. Passwords will never be stored in a clear text file. This includes storage of passwords in configuration files, database files, application code and system directories. Any such passwords must be encrypted if

they are required.

C. Passwords will never be sent via unsecured (i.e., unencrypted and unauthenticated) email.

D. Passwords will not be stored in written form (e.g. sticky notes) except if secured in an approved locked area.

E. All users should avoid using the "remember password" feature on web sites and other applications.

F. Passwords are never to be lent or divulged.

CHANGE MANAGEMENT STANDARDS

Employee Changes

When an employee is hired, terminated, or changes job descriptions/roles, the access settings to the IT system must be modified. The procedure for these changes are as follows:

1. The Manager initiates the change request (new account, modified access, or terminated account), by Exiting Interview/Seperation form to the Human Resources Department.

2. Human Resources notifes the IT Department.

3. The IT Department notifies the Human Resourcsource Department when request completed.

Periodic user system access level review is performed by the C.E.O., or designee, with the assistance of the IT vendor. In addition, the IT vendor performs access reviews monthly. Any needed changes such as access levels or access blockage are made immediately.

Termination of Employment

Should an employee resign or be terminated, all files on the PC become the property of Easy Et. Copying of such files for personal use is prohibited. In addition, the employee's user accounts are removed or inactivated from all required systems (such as EFS/Statewide Reporting System (SRS), email, Client Database(s), telephony system) immediately.

VIRTUAL PRIVATE NETWORK (VPN) STANDARDS

These standards provides guidelines for Remote Access via VPN connections to the T Easy Et Systems.

1. The approval authority for remote VPN Access rests with the IT Director or designee. The request for approval should be submitted to Contractor IT End- user's Director.

2. The IS User is responsible for selecting an Internet service provider (ISP), coordinating installation, installing any required software, and paying associated fees.

Additionally:

A. IS End-users with VPN privileges are responsible for ensuring that unauthorized personnel do not access Department internal networks.

i. VPN use is to be controlled using either a one-time password authentication, such as a token device, or a public/private key system with a strong pass phrase.

ii. VPN gateways will be set up and managed by Department.

iii. All computers connected to Department external networks via VPN or any other technology must use the most up-to-date anti-virus software that is the corporate standard. This includes personal computers.

iv. VPN users will be automatically disconnected from Department systems after 60 minutes of inactivity. The user must then log in again to reconnect to the network. Pings or other artificial network processes are not to be used to keep the connection open.

v. Users of computers that are not Department-owned equipment must configure the equipment to comply with the Department's VPN and network policies.

vi. Only approved VPN clients may be used.

The following policies should be reviewed and cross-referenced for details of protecting information when accessing the corporate network via remote access methods.

A. Information Technology Acceptable Use Policy

BACKUP STANDARDS

Easy Et must maintain backup copies of all critical data and systems so that they can be used to provide the continued availability and viability of these resources when these events occur. This standard provides procedures for backing up electronically stored data, operating system, database and application.

1. Easy Et maintains the responsibility for backing up all operating systems, data, applications and databases residing on servers and network equipment under our span of control in accordance with the guidance provided below.

2. All operating software and application software necessary to access, recreate, or generate the information must be backed up periodically. The frequency of backup will depend on the significance of the information and its frequency of change. The most current copy of backup media should be stored off-site. Procedures for recovery and restoration of the information should be documented.

3. The concept of performing backups of data files and programs is as fundamental as any concept in information technology. Backup procedures should include the following:

A. Maintaining a copy of backups off site at all times.

B. Access to back-up files shall be limited to those employees that it is appropriate.

C. Multiple copies of back-up files are recommended so as to not overwrite the most recent back-up.

D. Backing up systems on a daily basis.

E. Backing up all necessary data files and programs to recreate the operating environment

F. Storing the current copy of backups off organization premises.

G. Storing backup copies at an off-site location sufficiently distant from the data center to ensure their protection if the original system is destroyed.

H. Considering the ease of access and retrieval from the off-site storage location, including blockage by debris, transportation, and hours of operation.

I. Backing up the printed documentation and preprinted forms necessary for recovery.

J. Backing up on media that are compatible with the alternate computer system that will be used following a disaster, considering storage density, media type, and type of tape or disk drive.

K. Ensure that the following are stored at an off-site storage location:

• Source and object code for production programs,

• Master files and transaction files necessary to recreate the current master files,

• System and program documentation,

• Operating systems, utilities, and other environmental software, and

• Other vital records.

L. On a monthly basis prior to transporting the drive off site, IS Department or designee will have the Program Director or designee view to ensure that data has been backed up and confirmed by both IS Department or designee and Operations Director or designee.

M. On a monthly basis restoration of one data folder is performed by IS Department or designee as follows:

a. Open the Recovery software

b. Select file and/or folders that need to be recovered.

c. Restore data to its original location or other location as instructed.

d. Review for completeness by Operations Director or designee.

REPLACEMENT OF OBSOLETE HARDWARE & SOFTWARE STANDARDS

These standards define the requirement of data destruction from both hardware and software products

used by Easy Et when they are either replaced or recycled because they are obsolete and/or no longer needed.

1. Personal computer turn-in procedure. When Easy Et disposes of personal computers or servers, Easy Et must perform the following steps to ensure that all data is properly deleted.

A. Purge the hard drive of all applications except the operating system.

B. Purge the hard drive of all other documents.

2. This Section is in relation to the Health Insurance Portability and Accountable Act of 1996. (HIPAA). Please cross- reference the Health Insurance Portability and Accountability Act Of 1996 (HIPAA) Policy. HIPAA Security Procedures for PC or server relocation/disposal at covered HIPAA entities

Perform the following steps to ensure that all HIPAA data is properly deleted from surplus equipment.

A. When a PC or server is moved within the covered entity immediate location, the internal HD can be reformatted.

B. When a PC or server is surplused and/or moved outside of immediate location, the internal HD must be physically destroyed and safely disposed of by the Contractor. (Note: The objective is to make HD permanently unusable and unrecoverable).

C. Destroy all application software disks.

D. Data downloaded onto a data storage medium must be disposed of by reformatting as opposed to being erased or deleted.

E. Data storage medium must be reformatted a second time before the medium is reused or disposed of.

PROGRAM POLICIES

CONFIDENTIAL INFORMATION AND INFORMATION SHARING STANDARDS

The Confidential Information and Information Sharing Standards provides guidelines for the handling of confidential information and sharing with respect to the Easy Et Systems. The confidentiality policies are to protect the confidentiality, integrity, availability, and reliability of all data shared on the network. These policies are also intended to prevent accidental or intentional unauthorized disclosure, modification, or destruction of information by persons within or outside the agency. Additionally, it is the policy of the Easy Et's Information Systems to protect the confidentiality, integrity, availability, and reliability of all information technology resources used to support the delivery of services to clients served by contracted agencies. It is the policy of the Easy Et's Information Systems to preserve client rights to confidentiality, to implement and enforce the protection of the security of client personal

information, as well as compliance with Federal, State and Local ordinances, laws, rules, regulations, policies and procedures governing the confidentiality of data.
Confidential data include, but are not limited to: client names, medical history records, social security numbers and financial information.

1. Easy Et shall at all times respect the privacy rights of the person being served by Easy Et through any of its services as well as the privacy of the agency's administrative records.
2. Information shared on the network must be consistent with Federal, State and Local ordinances, rules, regulations, policies and procedures, including to Chapter 163 of the Florida Statutes, Intergovernmental Programs, Part VI, "Collaborative Client information systems."
3. Data may be shared with participating agencies only with client's valid consent.
4. State, Federal and County laws protect data collected and analyzed by Easy Et for its Information Systems. The unauthorized disclosure of any information that could be used directly or indirectly to identify clients is prohibited.
5. Client specific data (e.g., client's unique record number, exact date of birth or death and other personal identifying information) shall be released on a need-to-know basis and only with the client's valid consent unless specific provisions for such release are met according to state and federal statues.
6. Confidential information may be revealed after careful consideration indicates the presence of clear and present danger to an individual or to society, and then only to those who must be informed in order to reduce that danger.
7. Information about the agency's internal, personnel and/or administrative affairs may be discussed only with others on a "need to know" basis.
8. Aggregate data (data that is cumulative and not traceable to individual clients), may be shared with other agencies.
9. When providing services over the phone, Easy Et may obtain and document verbal consent. Clients have the right to decline providing valid consent. Easy Et would inform them of the consequences of not providing consent.
10. The client shall be informed of the purpose for collection of the information and of its use within the agency and/or within the community of participating agencies in client-information sharing collaboratives.
11. The client or the client's duly authorized agency shall have the right to correct the accuracy and

completeness of the client's record.

12. Written and oral reports should contain only information germane to the report. Every effort should be made to protect the person's privacy.

13. In writing or training, care should be taken that any clinical material used should be presented in such a way that the identity of the individual is not revealed.

14. When providing face-to-face services, clients must sign the appropriate consent forms before data can be entered into the appropriate Easy Et System. During the client intake in order to ensure the integrity of client information entered into the system, the person conducting the full (face-to-face) intake shall request that the client present proper identification (e.g., government issued documentation such as driving license, D.M. V I.D. card, resident alien card, or social security card). Lack of proper identification will not hinder or delay the intake process. A unique record number (URN) I.D. will be generated by the Automated System for each client. The URN will be used to coordinate services across authorized service providers and to generate an unduplicated client count.

HEALTH INSURANCE PORTABILITY AND ACCOUNTABILITY ACT OF 1996 (HIPAA) IT COMPLIANCE STANDARDS

This policy identifies the special handling of Electronic Personal Health Information (ePHI) as it applies to the IT resources throughout the Agency. The Health Insurance Portability and Accountability Act of 1996 (HIPAA) identifies and defines certain health plans, health care providers and health care clearinghouses ("Covered Entities") that must comply with its provisions. This policy's scope includes all electronic protected health information, as described in herein.

1. Administrative Safeguards. Employees, Shift Leaders, Managers and Directors shall work with the Director of HR & Administration to enforce laws and personnel rules related to the protection of data maintained by Easy Et and confidentiality of health information, with specific attention to the requirements of HIPAA. Employees shall be personally accountable if PHI is released in violation of HIPAA, and shall be subject to disciplinary actions according to existing personnel rules.

2. Technical Safeguards. Access Control and Integrity – Implement technical policies and procedures for electronic information systems that maintain ePHI to allow access only to those persons or software programs that have been granted access rights as specified in Sec. 164.308(a)(4).

A. Managers and Directors shall work with the Director of HR & Administration to make sure that only current, authorized staff has access to computer data where PHI is stored and used. All access to such

systems shall be password controlled, and rights to access shall be reviewed for each staff member at least annually.

B. Staff shall use password–protection on their voice-mail accounts. Staff shall not give out voice mail passwords to any non- Easy Et staff, and shall not post or keep passwords written down where they can be readily found by someone else (e.g. taped to desk, side of computer or telephone).

C. Staff shall protect access to their computer through the network log-in screen. Staff shall not share password with anyone, and shall not post or keep passwords written down where they can be readily found by someone else (e.g. taped to desk, side of computer, or telephone).

D. The IT Security Point of Contact shall be responsible for the deactivation and termination of User Accounts immediately following the notification from Human Resources or Directors regarding terminated workforce members.

E. Staff shall use the "Log-off" function to lock computers when away from their workstations.

F. Staff shall save electronic files on a secure computer. PHI shall not be saved onto diskettes, data tapes or CD (including Zip Disks or portable hard disks) unless absolutely necessary.

G. Staff shall orient their computer screens so they may not be easily seen by office visitors when displaying PHI.

H. Staff who uses laptops Personal Digital Assistants (PDAs) shall follow the same types of safeguards outlined for computer use. If the PDA contains confidential information (such as appointment information that may include PHI), the PDA must be safeguarded from being accessed by anyone outside of Contractor employees. If a PDA containing PHI is lost or stolen, a report shall be promptly filed with the Privacy Officer.

I. Staff shall destroy electronic media containing ePHI that does not have to be retained prior to disposal of the electronic media.

J. Staff shall ensure that all ePHI stored on Contractor computer hardware is encrypted and that there are plans to capture that ePHI in times of emergency.

K. Staff will audit computer hardware that hosts ePHI for compliance with the above Access Control requirements

3. Transmission Security guard against unauthorized access to ePHI that is being transmitted over an electronic communications network. (In the February 20, 2003 issue of the Health and Human Services Federal Register, the encryption required by Section 164.312(e)(1)) for ePHI was changed. Covered

entities are required to encrypt data being transmitted whenever deemed appropriate by the sending entity. However the section also recommends that covered entities consider use of encryption technology for transmitting ePHI when available, particularly over the internet.) Covered entities will be responsible for identifying transmission encryption requirements which will be implemented using appropriate encryption standards.

4. Reporting Suspected Violations. If a User suspects that another User has violated the Privacy Policies and Procedures, the User shall immediately report the suspected violation by using one of the following methods. Reporting the suspected violation is not optional. A report of the suspected violation may be given to:

A. A Director

B. HR and Admin Director

C. the IT Security Point of Contact.

Easy Et County Continuum of Care (CoC) Compliance

This agency is a partner in the Easy Et County FL-601 Continuum of Care (CoC) HMIS. Easy Et CoC HMIS partner agencies work together to provide services to persons and families who are experiencing homelessness. When clients request or receive services, we may collect data about clients and their households that may be shared with other Easy Et CoC HMIS partner agencies. Sharing their data allows service providers to see if they have housing services that fit your needs and for the purpose of ensuring effective coordination of services. It does not guarantee that clients will receive housing.

IMPORTANT: Do not enter personally identifying information into Homeless Management Information System (HMIS) for clients who are: 1) in Domestic Violence agencies or; 2) currently fleeing or in danger from a domestic violence, dating violence, sexual assault or stalking.

Who can have access to client information?

Agencies and/or organizations that participate in the HMIS Database can have access to client data. These agencies and/or organizations may include homeless service funders/providers, housing providers, healthcare providers, and governmental agencies. Additional agencies and/or organizations may join the Easy Et CoC HMIS at any time and will also have access to client data.

The Family Educational Rights and Privacy Act (FERPA) Compliance

The Family Educational Rights and Privacy Act (FERPA) (20 U.S.C. § 1232g; 34 CFR Part 99) is a Federal law that protects the privacy of student education records. The law applies to all schools that receive funds under an applicable program of the U.S. Department of Education.

FERPA gives parents certain rights with respect to their children's education records. These rights transfer to the student when he or she reaches the age of 18 or attends a school beyond the high school level. Students to whom the rights have transferred are "eligible students."

• Parents or eligible students have the right to inspect and review the student's education records maintained by the school. Schools are not required to provide copies of records unless, for reasons such as great distance, it is impossible for parents or eligible students to review the records. Schools may charge a fee for copies.

• Parents or eligible students have the right to request that a school correct records which they believe to be inaccurate or misleading. If the school decides not to amend the record, the parent or eligible student then has the right to a formal hearing. After the hearing, if the school still decides not to amend the record, the parent or eligible student has the right to place a statement with the record setting forth his or her view about the contested information.

• Generally, schools must have written permission from the parent or eligible student in order to release any information from a student's education record. However, FERPA allows schools to disclose those records, without consent, to the following parties or under the following conditions (34 CFR § 99.31):

o School officials with legitimate educational interest;

o Other schools to which a student is transferring;

o Specified officials for audit or evaluation purposes;

o Appropriate parties in connection with financial aid to a student;

o Organizations conducting certain studies for or on behalf of the school;

o Accrediting organizations;

o To comply with a judicial order or lawfully issued subpoena;

o Appropriate officials in cases of health and safety emergencies; and

o State and local authorities, within a juvenile justice system, pursuant to specific State law.

Schools may disclose, without consent, "directory" information such as a student's name, address, telephone number, date and place of birth, honors and awards, and dates of attendance. However, schools must tell parents and eligible students about directory information and allow parents and eligible students

a reasonable amount of time to request that the school not disclose directory information about them. Schools must notify parents and eligible students annually of their rights under FERPA. The actual means of notification (special letter, inclusion in a PTA bulletin, student handbook, or newspaper article) is left to the discretion of each school.
For additional information, you may call 1-800-USA-LEARN (1-800-872-5327) (voice). Individuals who use TDD may use the Federal Relay Service.

Or you may contact us at the following address:
Family Policy Compliance Office
U.S. Department of Education
400 Maryland Avenue, SW
Washington, D.C. 20202-8520
Collection of Social Security Numbers

The following information is pursuant to section 119.071(5), Florida Statues.

Social Security numbers of applicants and household members are requested because this information has been determined to be imperative for the performance of the duties and responsibilities prescribed by the law under Easy Et services which require this identifying information. This information is not required by state or federal law; however, social security numbers are necessary to determine eligibility for certain Easy Et program services and specifically for the following purposes:
1. To verify an applicant's identity.
2. To verify household size.
3. To verify household income.
4. To assist client apply for, obtain and maintain services for which they consent to apply.
A social security number collected pursuant to this notice can only be used by Easy Et for purposes specified above.

Nondisclosure except under limited circumstances.
Social security numbers will not be disclosed to others unless required or authorized by Florida law. Section 119.071(5), Florida Statues, allows disclosure of a person's social security number under the following specific, limited circumstances:
• If disclosure is expressly required by federal or Florida law or is necessary for the agency or

governmental entity to perform its duties and responsibilities;

• If the individual expressly consents to disclosure in writing;

• If disclosure is made to prevent and combat terrorism pursuant to the U.S. Patriot Act of 2001 or Presidential Executive Order 13224 (blocking property and prohibiting business transactions with persons who commit, threaten to commit, or support terrorism);

• For an agency employee and dependents, if disclosure is necessary to administer the person's health benefits or pension plan funds; or

• If disclosure is for the purpose of the administration of the Uniform Commercial Code by the office of the Secretary of State.

• If disclosure is requested by a commercial entity for permissible uses under the federal Driver's Privacy Protection Act of 1994, the federal Fair Credit Reporting Act, or the federal Financial Services Modernization Act of 1999 (for example, to verify the accuracy of personal information provided by the individual to the commercial entity; use by an insurer in connection with claims investigation or anti-fraud activities; for use in connection with a credit transaction).

REMOTE ACCESS STANDARDS

Easy Et grants remote access privileges to key staff. A list of staff and approved contractors granted. The same non-disclosure and confidentiality rules apply to all staff granted remote access privileges.

MOBILE COMPUTING DEVICE (AKA PORTABLE MEDIA STORAGE OR PERIPHERAL DEVICES) STANDARDS

Easy Et grants mobile computing device privileges to staff based upon duties/ responsibilities. A list of staff with mobile computing devices, which are password protected, is maintained by the individual responsible for Inventory Control. The same non-disclosure and confidentiality rules apply to all staff granted mobile computing device privileges. Mobile computing devices are inspected at least annually, more frequently if warranted, to ensure that the device continue to be password protected and that no confidential data is stored on the hard drive. The inspection is documented on a Protecting Mobile Computing Device form, which is retain in accordance with Records Retention policies. Easy Et prohibits the use of mobile computing devices (flash drives, thumb drives, laptops, email transmissions, etc.) that are unencrypted or lack activated password protections.