HUMAN SERVICES DEPARTMENT

Information Systems Security Policies

Table of Contents

1. INTRODUCTION

- 1.1 Purpose
- 1.2 Scope
- 1.3 Objectives
- 1.4 References
- 1.5 Security Policies

2.0 ADMINISTRATIVE POLICIES

- 2.1 Information Security Awareness Policy
- 2.2 IT Security Incident Handling Policy
- 2.3 IT Security Risk Assessment Policy
- 2.4 IT Acceptable Use Policy
- 2.5 Information Classification Policy
- 2.6 Audit Policy
- 2.7 Security Administration Policy
- 2.8 Physical Security Policy
- 2.9 Contractor IT Security Program Policy

3.0 TECHNICAL POLICIES

- 3.1 Password Policy
- 3.2 Virtual Private Network (VPN) Policy
- 3.3 Backup Policy
- 3.4 Replacement of Obsolete Hardware & Software Policy
- 3.5 HIPPA of 1996 IT Compliance Policy

4.0 PROGRAM POLICIES

- 4.1 Confidential Information and Information Sharing Policy
- 4.2 Electronic Referral Policy

5.0 GLOSSARY

6.0 APPENDICES

Information Systems Security Policies

1.0 Introduction

Policies are high-level statements that provide individuals with a basis for making decisions about the operations of an organization.

The Human Service Department ("Department") runs major Information Technology (IT) systems. The nature of services provided or contracted by the Department requires that client confidentiality and privacy rights are adequately protected. Additionally, a high level of need exists for exchanging data between agencies in order to make decisions. Thus, these security policies have been developed for the aforementioned purposes and comply with the Broward County Board of County Commissioners and Office of Information Technology.

1.1 Purpose

The purpose of these security policies is to inform Human Service Department ("Department") Client Services Management System (CSMS), ECHO, PICS, BIN (all hereinafter referred to as "Automated Systems") end-users, customers, contractors, non-profits, administrators, staff, and managers (all hereinafter referred to as "Users") of their obligation to protect the County's infrastructure and information assets. Contractors include any agency that maintains a contract, interlocal agreement or memorandum of understanding with the Department or who subcontracts with an agency which maintains a contract or memorandum of understanding with the Department. Staff includes all staff of the Department and staff of any Contractor. The policies specify the DOs and DON'Ts necessary to follow security implementation best practices.

A secondary purpose of these policies is to provide a guideline for audit compliance of computer and systems and networks and compliance with the Department.

1.2 Scope

IT Security is the responsibility of every Information Systems User. As such, all Department Information Systems Users must be informed of the information technology security policies. Contractors must implement the policies defined in this document. Contractor-level policies must be based on the high-level policy statements presented in this document.

It is the policy of Department that:

- Department information resources are valuable assets of the Department and, as such, must be protected to some degree from unauthorized disclosure, modification, or destruction, whether accidental or intentional. Determining the degree of protection of assets and implementing appropriate controls is a management function from the Contractor.
- Electronic protected health information shall be protected following the Health Insurance Portability and Accountability Act of 1996 (HIPAA) Policy as outlined herein.
- In the event a disaster or catastrophe disables information processing functions, the ability to continue critical Contractor services must be assured.
- Security controls required by law must be complied with and Department 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.
- Consequences of non-compliance with these Policies can include: suspension of access privileges, and breach of contract for cause.

1.3 Objectives

The objectives of this document are to establish Department-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 department 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 and IS User to make good decisions about information security
- Coordinate efforts of Department contracted providers to provide consistent information.

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

1.4 References

County Administrative Code, the OIT Handbook and the Health Insurance Portability and Accountability Act of 1996 (HIPAA) were used in the preparation of this document.

1.5 Security policies

Policies are grouped into three categories:

- Administrative
- Technical
- Program

2.0 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.

2.1 Information Security Awareness Policy

Policy purpose

This Policy 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 hereto as Exhibit A) to any Department Automated System. This will also ensure that IS Users are aware of information security threats and concerns, and are equipped to support the Department's IT security policies in the course of their normal work.

Policy Scope

The policy establishes the requirement for security awareness and education of all IS Users that are granted access to the Department'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.

Policy Description

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:

- All Contractors shall ensure that their IS users under their supervision are aware of the Department's current IT security policies.
- All Contractors 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.

2.2 IT Security Incident Handling Policy

Policy purpose

This policy describes the procedure for dealing with computer security incidents and provides Department support personnel 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.

Policy Scope

The term incident in this policy is defined as any irregular or adverse event that occurs on any part of the Human Service Department 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.

Policy Description

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 the Contractor's local administrator who in turn should report to the Department IT Information Systems Manager. IS Users should not attempt to prove a suspected weakness as testing weaknesses might be interpreted as a misuse of the system.

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 fours 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.

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.

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.

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 the Contractor
- People Contractor has contacted or have contacted Contractor
- Names of systems, programs or networks that have been affected

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 the System

  Isolate infected system(s) from the remaining Department network as soon as possible. If a worm is suspected, then a decision must be made to disconnect the Department from the outside world. Network isolation is one method to stop the spread of a worm, but the isolation can also hinder the clean-up effort since the Department will be disconnected from sites which may have patches. The Department Information Systems Manager or designee must authorize the isolation of the Department 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.
- Identify the Problem

  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. Below is a list of tasks to make a snapshot of the system:

- Save a copy of all system log files.
- Save a copy of the root history file.
- 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 Department 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.**

2.3 IT Security Risk Assessment Policy

Policy purpose

This policy places the accountability and responsibility of performing IT security risk assessment on Contractor applications/systems administrators. The purpose of the risk assessment is to determine areas of vulnerability, and to initiate appropriate remediation.

Policy scope

IT security risk assessments can be conducted on any Contractor that maintains an agreement or memorandum of understanding with the Department.

IT security risk assessments can be conducted on any information systems, including applications, servers, and networks, and any process or procedure by which these systems are administered and/or maintained.

Policy description

An initial IT security risk assessment must be performed on every critical business application/system by the Contractor applications/systems administrator. The execution, development and implementation of remediation programs are the joint responsibility of the Contractor and the Department. Contractor users and employees are expected to cooperate fully with any Risk Assessment being conducted on systems for which they are held accountable. Users and employees are further expected to work with the Risk Assessment Team in the development of a remediation plan.

2.4 Information Technology Acceptable Use Policy

Policy purpose

The purpose of this policy is to outline the acceptable use of Human Service Department Automated Systems assets and resources. This policy is intended to protect the Department from risks including virus attacks, compromise of network systems and services, and legal issues.

Policy scope

This policy applies to Contractor's which contract with the Department, its users and customers and pertains to all IT assets and resources owned or leased by the Department.

Policy description

Department Information Technology assets and resources are provided primarily for the use of Contractors which contract with the Department. Appropriate use of these resources includes conducting Department business, research, communications, and official work. Access to Department IT assets and resources is a privilege. It requires individual users and employees of Contractor's to act responsibly, conserve computer resources, and consider the rights and privacy of others. The assets and resources are the property of the Department.

Users and employees of Contractors 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. Contractors are responsible for ascertaining, understanding, and complying with the laws, rules, policies, contracts, and licenses applicable to their particular uses.

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.

The Department reserves the right to monitor computer and network usage for operational needs and to ensure compliance with applicable laws and Department policies.

2.5 Information Classification Policy

Policy purpose

This policy identifies the different classifications of information within the Department and defines classifications on how that information is to be handled and protected. It is also intended for the policy to help users and employees of Contractors to determine what information can be disclosed to non-employees, as well as the relative sensitivity of information that should not be disclosed outside of the Contractor or the Department without proper authorization.

Policy scope

This policy pertains to all information collected, stored and/or generated by Contractor in the use of Department Automated Systems.

Policy Description

All information, data and documents is to be processed and stored strictly in order to protect its integrity and confidentiality

Sensitive Information

Sensitive Information is defined as, for purposes of defining Contractor-produced software, only those portions of data processing software, including the specifications and documentation, which are used to:

A. Collect, process, store, and retrieve information.
B. Collect, process, store, and retrieve financial management information of the provider agency, such as payroll and accounting records; or
C. Control and direct access authorizations and security measures for automated systems.
D. Medical history records, including HIPAA ePHI[1] and information related to health or property insurance.

2.6 Audit Policy

Policy purpose

This policy provides the authority for members of the Department to conduct security audits.

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.

Policy scope

This policy covers any system or equipment on or connected to the Department Automated Systems. Department staff may conduct security audits on other Department owned/operated networks as tasked by the Department Director.

Policy description

When requested and for the purpose of performing an audit, any access needed for the audit will be provided to members of the 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 Department networks.

[1] Health Insurance Portability and Accountability Act of 1996 electronic Personal Heath Information (see Health Insurance Portability and Accountability Act Of 1996 (HIPAA) IT Compliance Policy)

2.7 Security Administration Policy

Policy purpose

This policy defines security administration responsibilities for Contractors.

Policy scope

This policy covers all computer and communication devices on the administrative network owned or operated by the Contractor. 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 Department's information assets.

Policy Description

Security administration is an important function in the Department. Security administration responsibilities should be segregated from systems development, computer operations, and systems programming functions. 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.

Contractors will adopt proper security measures and procedures to protect the Department's information assets from all threats. These measures include establishing and assigning security administration authority and responsibility.

Contractors

A. Assign an IT Security Point of Contact who is responsible for controlling and monitoring physical and electronic access to Contractor specific information assets.
B. Ensure the ongoing protection of Contractor 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 online access to the automated systems within the Department.
C. Ensure that all staff adheres to the security policies, guidelines and procedures.
D. Involve the Department in security evaluations for Contractor specific information assets.

Department IT Security Administration

A. Provide orientation and support to the Contractor's IT Security Point of Contact.
B. Create and enforce security policies.
C. Ensure that password security functions, features, and capabilities are activated for online systems.
D. Set up user profiles (e.g., identification, authorization, user code, and password).
E. Ensure that passwords are of sufficient length and complexity that they cannot be easily compromised.
F. Limit the number of log-on attempts to online systems. No more than three to five attempts should be allowed before disabling the violator's workstation.

G. Ensure that passwords are changed for all online users at least every 90 days. Users with more sensitive capabilities (e.g., security administrators, certain users of financial and payroll systems) may want to change their passwords more frequently.
H. Establish adequate password security on automated systems.
I. Review terminal logs and security violation reports.
J. Monitor activity on remote access facilities to ensure that only authorized personnel are using them.
K. Detect and monitor access to systems or information outside the normal patterns or needs of a user or specific workstation.
L. Maintain security over Department information to ensure that unauthorized access does not occur.
M. Report potential security breaches to Contractor Management. Monitor and track repeated security violators.
N. Maintain historical records of security violations for at least 90 days.
O. Provide suggestions and recommendations to the Department on security-related matters.
P. Research and suggest, as requested, additional security devices, such as modems with dial-back capability, which can potentially improve security.
Q. Closely monitor the following:
    1. Individuals with access to any tool that can change programs or data, such as program compilers, data-altering utilities, report generators, and text editors.
    2. Remote access lines, especially those with dial-up and VPN capabilities.
    3. Terminated employees, especially those with high-tech capabilities.
    4. Repeat violators who claim not to understand log-on procedures.

All IS End-users

A. Adhere to all established security policies.
B. 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.
C. Refrain from sharing confidential user codes, passwords, or other codes intended to restrict access to information assets.

2.8 Physical Security Policy

Policy purpose

Authorized access to computer facilities is granted on a "need-to-use" basis.

Policy scope

This policy applies to all Contractors which contract with the Department.

Policy description

This policy 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.

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 Department Information Systems Manager or designee should be contacted for assistance in developing plans for physical security of IT facilities.

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.

Physical entry controls

Secure areas should be protected by appropriate entry controls to ensure that only authorized personnel are allowed access. The following controls should be considered:

A. Visitors to secure areas should be supervised and their date and time of entry and departure recorded.
B. Visitors should only be granted access for specific, authorized purposes.
C. All personnel are required to wear visible identification when within the secure area and encouraged to challenge strangers.
D. Access rights to secure areas should be revoked immediately for personnel that terminate employment.
E. Any keys or other access devices issued to the employee must be returned as part of the termination process.

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. Key facilities should be situated away from areas of public access or direct approach by public vehicles.
B. 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.
C. Lobby directories and internal telephone books should not identify locations of computer facilities.
D. Backup equipment and media should be situated at a safe distance to avoid damage from a disaster at the main site.
E. 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.
F. Emergency procedures should be fully documented and regularly tested.
G. Doors and windows should be locked when unattended, and external protection should be considered for windows.

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.

2.9 Contractor IT Security Program Policy

Policy purpose

The purpose of this policy is to ensure that each Contractor which contracts with the Department understands that they must establish, implement and continuously improve an IT Security Program. This program must be sufficient enough to guarantee the integrity, accuracy and availability of information for which they have custodial responsibility. The program must reduce the risk of unauthorized disclosure, modification or destruction of information to a level that management deems necessary. Managers will be held accountable.

Policy Scope

This policy covers each Contractor which contracts with the Department.

Policy Description

Each Contractor will appoint an IT Security Point of Contact (IT Security POC) as an additional duty. The IT Security POC will work directly with the Department Information Systems Manager in developing and monitoring the program. The following skills/competencies are recommended to be included in the IT Security POC:

A. A working knowledge of all business processes and information handled by those processes.
B. A knowledge of the level of risk associated with the loss or destruction of the some or all the information for which the Contractor has custodial responsibility.
C. Excellent written and verbal communications skills.
D. Willingness to be an active partner with the Department Information Systems Manager in raising the level of Security within the entire Contractor.

Each Contractor which contracts with the Department must develop a comprehensive Security Program that allows them to:

A. Ensure the accuracy and integrity of automated information, and
B. Educate all employees and contractor personnel concerning their responsibilities for maintaining the security of information resources.

Additionally, it is recommended that the comprehensive Security Program include the following:

A. Place a monetary value on all data, software and information system resources owned by the Contractor for risk management purposes.
B. Identify which information resources are sensitive and take steps to protect such information from disclosure or unauthorized modification.
C. Identify which information resources are essential to the continued operation of critical County functions and take steps to ensure their availability.
D. Evaluate IT Security enhancements beyond the minimum requirements for their cost effectiveness and to apply those which can be cost justified considering the exposure.

3.0 Technical Policies

The following policies are technical in nature and must be implemented by all Contractors which contract with the Department.

Access to information and resources available through the Department'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.

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

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

The following policies should be read and cross referenced as part of the Broward County's Network Security.

A. Backup Policy
B. HIPAA IT Compliance Policy
C. Password Policy

In support of these policies, the 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.

3.1 Password Policy

Policy purpose

This policy outlines the handling, responsibilities, and scope of passwords for the Automated Systems.

Policy scope

This policy includes all Contractors which contract with the Department who access to the Department Automated Systems.

Policy description

All Contractor users and employees authorized to access password protected data on Department systems must complete the appropriate User Access Form. Passwords shall be controlled to prevent their disclosure to unauthorized persons. Contractors shall control their passwords to prevent their disclosure to unauthorized persons.

Passwords for **all** systems are subject to the following rules:

A. All passwords must be changed every ninety days.
B. Passwords must not be inserted into e-mail messages or other forms of electronic communication.
C. No passwords are to be written, e-mailed, hinted at, or in any way shared with anyone.
D. Passwords are not to be displayed or concealed on your workspace.
E. All systems "Guest" accounts are to be disabled, and any newly created "Temp" accounts to have a limited "life expectancy" with an option for authorized extension.
F. Password must meet the following criteria:

1. May not contain any part of the user's account name.
2. Must be least 8 alpha-numeric characters long.
3. Only 5 failed attempts will be allowed before account is locked.
4. A user will not be allowed to reuse the password for 15 consecutive change cycles. (System will remember last 15 passwords).

The Backup policy should be read and cross referenced as part of the Department Automated Systems Security.

3.2 Virtual Private Network (VPN) Policy

Policy purpose

This policy provides guidelines for Remote Access via VPN connections to the Department Automated Systems.

Policy scope

This policy applies to all Contractors which contract with the Department using VPNs to access the Automated Systems. This policy applies to all implementations of VPN access.

Policy description

The approval authority for remote VPN Access rests with the Contractor IT End-user's Director and the Department Information Systems Manager or designee. The request for approval should be submitted by the Contractor IT End-user's Director on the appropriate User Access Form. The form should be forwarded to the Department Information Systems Manager or designee.

Approved Department IT Contractors may use the benefits of VPNs, which are a *user managed* service. 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.
B. 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.
C. VPN gateways will be set up and managed by Department.
D. 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.
E. 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.
F. Users of computers that are not Department-owned equipment must configure the equipment to comply with the Department's VPN and network policies.
G. 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
B. Dial-in Access Policy

3.3 Backup Policy

Policy purpose

This policy provides procedures for backing up electronically stored data, operating system, database and application.

Policy scope

This policy applies to all Contractors which contract with the Department.

Policy description

Contractors maintain the responsibility for backing up electronically stored data, operating systems, databases and applications.

Contractors are responsible for backing up all data, or work group applications and database stored on their desktops laptops and any Personal Digital Assistant (PDA). This data can be backed up on network shared drives (preferred), compact disks or floppy disks.

Contractors are responsible for backing up all operating systems, data, applications and databases residing on servers and network equipment under their span of control in accordance with the guidance provided below.

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.

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. Backing up systems on a daily basis.
C. Backing up all necessary data files and programs to recreate the operating environment
D. Storing the current copy of backups off organization premises.
E. Storing backup copies at an off-site location sufficiently distant from the data center to ensure their protection if the original system is destroyed.
F. Considering the ease of access and retrieval from the off-site storage location, including blockage by debris, transportation, and hours of operation.
G. Backing up the printed documentation and preprinted forms necessary for recovery.
H. Having at least three generations of backup tapes so an earlier generation of backup can be used if the current backup media are damaged or become unreadable.
I. Ensuring that backup is not continually performed on the same set of tapes.
J. Testing the backup to determine if data files and programs can be recovered.
K. 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.
L. 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.

3.4 Replacement of Obsolete Hardware & Software Policy

Policy purpose

This policy defines the requirement of data destruction from both hardware and software products used by the Contractor when they are either replaced or recycled because they are obsolete and/or no longer needed.

Policy scope

This policy applies to all Contractors which contract with the Department.

Policy description

Personal computer turn-in procedure

When a Contractor disposes of personal computers or servers, the Contractor 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.

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) IT Compliance Policy contained within this document.

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.

3.5 Health Insurance Portability and Accountability Act Of 1996 (HIPAA) IT Compliance Policy

Policy purpose

This policy identifies the special handling of Electronic Personal Health Information (ePHI) as it applies to the IT resources throughout the Department. This policy must be used when establishing the individual Contractor IT Security Program. 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.

Policy Scope

This policy is applicable to all Contractors that use or disclose electronic protected health information for any purposes. This policy's scope includes all electronic protected health information, as described in herein.

Policy Description

Administrative Safeguards

Contractor managers, and supervisors shall work with its Human Resource section to enforce laws and personnel rules related to the protection of data maintained by Department and confidentiality of health information, with specific attention to the requirements of HIPAA. Contractor employees shall be personally accountable if PHI is released in violation of HIPAA, and shall be subject to sanctions according to existing personnel rules.

Technical Safeguards

A. 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).

1. Contractor administrators, managers and supervisors shall work with the Department 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.
2. Contractor staff shall use password–protection on their voice-mail accounts. Contractor staff shall not give out voice mail passwords to any non-Contractor 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).
3. Contractor staff shall protect access to their computer through the network log-in screen. Contractor 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).
4. The Contractor's IT Security Point of Contact shall be responsible for notifying Human Resources section of the Contractor and the Department Information Systems Manager regarding terminated workforce members by requesting the deactivation of the individual's passwords. Access shall be terminated immediately following notification.
5. Contractor staff shall use the "Log-off" function to lock computers when away from their workstations.
6. Contractor 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.
7. Contractor staff shall orient their computer screens so they may not be easily seen by office visitors when displaying PHI.
8. Contractor staff who uses 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.
9. Contractor staff shall destroy electronic media containing ePHI that does not have to be retained prior to disposal of the electronic media.
10. Contractor 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.
11. Contractor staff will audit computer hardware that hosts ePHI for compliance with the above Access Control requirements
12. Contractor staff will implement electronic mechanisms to corroborate that ePHI has not been altered or destroyed in an unauthorized manner.

B. 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.

Reporting Suspected Violations

If a Contractor staff member suspects that another employee of Contractor has violated the Privacy Policies and Procedures, the Contractor staff member 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 the Contractor's IT Security Point of Contact.

4.0 Program Policies

4.1 Confidential Information and Information Sharing Policy

Policy purpose

This policy provides guidelines for the handling of confidential information and sharing with respect to the Department Information 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 participating agencies. Additionally, it is the policy of the Department'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 participating member agencies. It is the policy of the Department'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.

Policy scope

This policy applies to all Contractors which contract with the Department and use Department Automated Systems and to Department staff. Confidential data include, but are not limited to: client names, medical history records, social security numbers and financial information.

Policy description

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."

Data may be shared with participating agencies only with client's valid consent. This data may not be shared with any individual or organization that does not have a current signed agreement with the participating agency. The minimum data elements to be collected by participating agencies, as required by funding agencies are as follows: name, alias and zip code, if applicable, gender, and date of birth and social security number.

State, Federal and County laws protect data collected and analyzed by Department for its Information Systems. The unauthorized disclosure of any information that could be used directly or indirectly to identify clients is prohibited.

Client specific data (e.g., client's unique record number, exact date of birth or death and other personal identifying information) shall be released to participating agencies on a need-to-know basis and only with the client's valid consent.

Aggregate data (data that is cumulative and not traceable to individual clients), may be shared among participating agencies.

Clients must sign the appropriate consent forms before data can be entered into the appropriate Automated System, except only that Contractor's performing central intake via telephone may obtain verbal consent. In the event that the potential client declines to provide valid consent, the client intake process will be completed manually or by other previously approved methods.

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.

4.2 Electronic Referral Policy

Policy purpose

This policy provides guidelines for the handling of electronic referrals with respect to Department Information Systems.

Policy scope

This policy applies to all Contractors which contract with the Department and use the Department Information Systems and Department staff.

Policy description

Electronic Referrals to participating member agencies that provide services, for which the client may be eligible, will be done electronically via the appropriate Department Automated System. If the Contractor that the client is being referred to is a Department Automated Systems participating agency, the information will be received by that agency electronically, subject to valid client consent. All printed materials generated by the appropriate Department Automated System are considered confidential. This includes confidential client information relative to demographics, annual household income, financial assistance and service outcomes. This printed material may be faxed or mailed to that agency in accordance with all applicable Federal, State and County laws.

5.0 Glossary

Terms	Definitions
Covered Entities	Organizations that are directly regulated by HIPAA and are responsible for the privacy of protected health information.
Desktop	PCs and peripheral equipment are not relevant to the scope of this policy.
Electronic Protected Health Information (ePHI)	Electronically stored or transmitted Protected Health Information.
Encryption	Secure Broward County sensitive information in accordance with the Acceptable Encryption Policy. International issues regarding encryption are complex. Follow organization guidelines on export controls on cryptography, and consult your manager and/or organization legal services for further guidance.
Hypertext transfer protocol (HTTP)	A protocol that tells computers how to communicate with each other. Most Web page locations begin with http://.
Internet	A global network of computers that communicate using a set of common protocols including hypertext transfer protocol (HTTP) and Transmission control protocol/ Internet protocol (TCP/IP). A private global network inside a company or organization that uses the same kinds of software that you would find on the public Internet, but that is only for internal use. Note that an Intranet may not actually be an internet – it may simply be a network.
Internet service provider	This is the organization that the County contracts with to get connection to the Internet.
Intranet	An private network of computers that communicate using a set of common protocols including hypertext transfer protocol (HTTP) and Transmission control protocol/ Internet protocol (TCP/IP).
One-time password authentication	The use of a one-time password token to connect to a network over the Internet.
Personal digital assistant (PDA)	Personal digital assistant.
Point of contact (POC)	Point of contact - The POC acts on behalf of the Contractor.
Protected Health Information (PHI)	Individually identifiable health information that is: transmitted by electronic media, maintained in electronic media, or transmitted or maintained in any form or medium. Protected health information excludes individually identifiable health information in: education records covered by the Family Educational Rights and Privacy Act; and in employment records held by a covered entity in its role as employer.
Risk	Those factors that could affect confidentiality, availability, and integrity of Broward County's key information assets and systems.
Risk assessment	Periodic information security assessments for the purpose of determining areas of vulnerability and to initiate appropriate remediation.

Terms	Definitions
Transmission control protocol/Internet protocol (TCP/IP)	The suite of transmission protocols that are used across the Internet.
Virtual private network (VPN)	An encrypted channel between nodes on the Internet. The provision of private voice and data networking from the public switch network through advanced public switches. The network connection appears to the IT Customer as an end-to-end, nailed-up circuit without actually involving a permanent physical connection, as in the case of a leased line. VPNs retain the advantage of provide networks but add benefits like capacity on demand.

6.0 Appendices

Exhibit A

Client Services Information Systems

User Confidentiality Security Agreement

I, the undersigned, have received and read a copy of the Broward County Human Services Department Information Systems Security Principles and Policies. I hereby agree to abide by these principles and policies.

I acknowledge that violation of the Principles and Policies may result in criminal prosecution, civil liability, civil penalty and may subject me to disciplinary action, including possible termination of employment.

I understand that the purpose of this agreement is to emphasize that all client information contained in any of the Department's client services systems is confidential.

I understand my professional responsibilities, and that I am to report suspected or known security violations to Broward County Human Services Department.

I understand that access to confidential information is governed by State and Federal laws. Client confidential information includes medical, social and financial data.

Client data collected by interview, observation or review of documents must be in a setting which protects the client's privacy.

I further understand and acknowledge the following:

1. Registered user ID's and/or passwords are not to be disclosed.
2. Information, electronic or paper-based, is not to be obtained for my own or another person's personal use.
3. Client services information systems, data and information technology resources shall be used only for official business purposes.
4. Copyright law prohibits the unauthorized use or duplication of software.

User Name: _____

(print)

User Signature: _____ Date Signed: _____

Agency: _____

Supervisor Name: _____

(print)

Supervisor Signature: _____ Date Signed: _____