

APPENDIX H SECURITY PLAN CHECKLIST

Security Plan Checklist Overview

The SPC is meant for technical reviewers/developers of security plans in State health and human services agencies; based on guidance from NIST*, FIPS*, and USDA/FNS. Not all items on the SPC are mandatory, but each major section should be addressed in some form or another.

The purpose of Security Plan Checklist is to assist the State in protecting agency information and information processing assets from theft, fraud, misuse or unauthorized modification. Information used by any business enterprise must be safeguarded against tampering, loss, unauthorized disclosure, denial of service, destruction and must be available when and where needed.

In accordance with the NIST Handbook (*Introduction to Computer Security*), there are four major IT security Controls that should be addressed:

1. Management Controls
2. Operational Controls
3. Technical Controls
4. Electronic Benefits Transfer (EBT) Specific Controls [reserved for future use]

Each of the controls has related security subgroups in this checklist. Use of the checklist during development or upgrade of an MIS will provide the State with a basic understanding of what security controls should be put into place, and provide guidance on further development, as well as maintaining a secure computing environment.

*NIST- National Institute of Standards and Technology

*FIPS – Federal Information Processing Standards

SYSTEM IDENTIFICATION	
	System Name and Title
	Responsible Organization (organization responsible for system operation)
	System Owner (name, title, agency, address, phone number, email address)
	Authorizing Official (senior management official who has authority to accredit the system and accept residual risk associated with the system)
	Designated Points of Contact (other key personnel who can address system information)
	Assignment of Security Officer (individual responsible for the system security)
	System Category (major application or general support system)
	Your application category(ies) and how they are integrated with your system are described. I. Information access - hypertext, multimedia, soft content and data II. Collaboration – newsgroups, shared documents, videoconferencing III. Transaction processing – internet commerce or business, links to legacy systems
	System Status (under development, operational, or undergoing a major modification)
	General Description/Purpose (brief description – one to three paragraphs – of the function and purpose of the system)
	Functions you are using the internet to perform are described (data transfer, forms-based data entry, browser-based interactive applications, etc.)
	System Environment (brief description of the technical system including any environmental or technical factors that raise special security concerns, such as PDA's, wireless technology, etc.)
	System Interconnection/Information Sharing (list each system interface or interconnection) I. Name of system II. Organization III. Type of interconnection (internet, dial-up, etc.) IV. Authorizations for interconnection (MOU/MOA, etc.) V. Date of agreement VI. Name and title of authorizing official(s)

SENSITIVITY OF INFORMATION HANDLED	
	The degree of sensitivity of information/data generated or accessed by the system is described, considering the requirements for: <ol style="list-style-type: none"> I. Confidentiality – Preserving authorization restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information. II. Integrity – Guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity. III. Availability – Ensuring timely and reliable access to and use of information.
	Minimum safeguards for protecting Personal Identifiable Information (PII) as required by the Office of Management and Budget guidance for protecting PII in memoranda M-06-15 and M-06-16 , “Protection of Sensitive Agency Information” are described
	Identify and describe the following information sensitivity elements: <ol style="list-style-type: none"> I. Applicable laws and regulations that require protection of sensitive information II. A description of the data sensitivity III. Data protection requirements for integrity, confidentiality, and availability
	System Security Measures –The system security measures in-place or planned that is intended to meet the protection requirements of the system. Security control measures should also be explained in general terms regarding the system are described.
MANAGEMENT CONTROLS	
Focus on the management of the information system and the management of risk for a system. They are techniques and concerns normally addressed by management driven by policy and process. (Identify and document the processes and procedures for the following)	
	Develop security policy and procedures that ensure system security
	Establish configuration controls for reviewing and approving security changes made to the system hardware, software, and application(s)
	Create procedures for reporting security incidents or irregularities (e.g., virus, hackers, software bugs)
	Designate a security manager responsible for overseeing the security program.
	Assign responsibility for computer security at each office or site.
	Ensure security activities are incorporated into the security program, including: <ol style="list-style-type: none"> I. Incorporate security specifications in the system design documents II. Conduct risk assessments and system security reviews. <ol style="list-style-type: none"> a. Ensure the risk analysis measures vulnerability related to fraud or theft or loss of data and harm to agency activities. b. Ensure risk analyses are conducted whenever there is a significant change to the physical facility, hardware, or operating system and application software. III. Develop appropriate security documentation such as contingency plans, risk assessment report, security plan and updates as required. IV. Ensure corrective actions are effectively implemented

	Develop and use change control procedures as programs progress through testing to final approval
	Determine the owner of sensitive or confidential data. Periodically verify with the owner of the data who has access to this data.
	Develop and enforce privacy policies for employees
OPERATIONAL CONTROLS	
Address security methods focusing on mechanisms primarily implemented and executed by people (as opposed to systems). These controls are put in place to improve the security of a particular system (or group of systems). They often require technical or specialized expertise and rely upon management activities as well as technical controls.	
<i>Personnel Security</i>	
	Duties are separated to ensure individual accountability
	Distinct systems support functions are performed by different individuals
	A process is developed and enforced for requesting, establishing, issuing, and closing user accounts. <ul style="list-style-type: none"> I. Security is notified within a reasonable period of time of the termination and hiring of employees. II. User accounts for terminated employees are closed with access rights deleted within a specific (short) period of time. III. User accounts for new hires are opened and access granted according to supervisory designated rights within a specific (short) period of time. IV. When an employee is terminated, access is denied to the system and any data, program listings, procedure manuals, and other employees are informed of the termination. V. Manager periodically reviews authorized users and their access authorities, making necessary changes.
	The delegation and maintenance of user access and passwords is limited to a select number of people
<i>Physical and Environmental Protection</i>	
	Access to facilities is controlled through the use of guards, identification badges, or entry devices such as key cards or biometrics
	Visitor access to facilities is controlled and monitored
	Management regularly reviews the list of persons with physical access to sensitive facilities
	Deposits and withdrawals of storage media authorized and logged
	Appropriate fire suppression and prevention devices are installed and working
	Emergency procedures are documented and employees are familiar with the procedures
	Computer monitors are located to eliminate viewing by unauthorized persons
	Physical access to data transmission lines is controlled
	Sensitive data files are encrypted on all portable systems
	Portable systems are stored securely
	Equipment located in areas accessible to clients and/or the public are properly secure to prevent tampering or accidental interruption of service

	Telecommunications closets and/or server areas are secured at all times
	The system automatically logs off a user after a specified period of inactivity
	Users logoff or turn off their computers/workstations when they will be away from an extended period of time
	Computers/workstations, servers and telecomm closets are kept clean and free of dirt, dust, and food
	Components are protected by surge protectors or line conditioners
	A Uninterruptable Power Supply (UPS) is available and tested periodically
	Users receive periodic training on emergency procedures and good housekeeping practices
	<i>Configuration Management</i>
	Organization develops, documents, and maintains under configuration control a current baseline configuration of the information system.
	Organization determines the types of changes to the information system that are configuration controlled; approves changes to the system with explicit consideration for security impact analysis; documents approved changes, retains and reviews records of changes, audits activities associated with changes, and coordinates and provides oversight for configuration change control activities through committee or board that convenes on a regularly defined basis.
	Organization conducts security impact analysis of changes to the system to determine potential security impacts prior to change implementation.
	Organization establishes and documents mandatory configuration settings for information technology products employed within the information system using defined security configuration checklists.
	Organization configures the information system to provide only essential capabilities and specifically prohibits or restricts the use of a defined set of prohibited or restricted functions, ports, and/or services.
	Organization develops, documents, and implements a configuration management plan for the information system that addresses roles, responsibilities, and configuration management processes and procedures.
	<i>Input/Output Controls</i>
	There is a help desk or group that offers advice and assistance
	Processes exist for the handling, distributing, and storing of output containing sensitive information
	Processes exist to ensure that unauthorized individuals cannot read, copy, alter, or steal printed or electronic information
	<i>Contingency Planning</i>
	Critical data files and operations are identified and the frequency of file backup documented
	Processing priorities been established and approved by management
	A comprehensive contingency plan been developed and documented
	There are detailed instructions for restoring operations
	There is an alternate processing site. (Identify location)

	The location of stored backups is identified
	Backup files are created on a prescribed basis and rotated off-site often enough to avoid disruption if current files are damaged
	System and application documentation is maintained at the off-site location
	The backup storage site and alternate site are geographically removed from the primary site. They are physically protected
	Tested contingency/disaster recovery plans are in place.
	The plan is periodically tested and readjusted as appropriate
	An incident response policy and procedure is defined, documented, and implemented
	Organization trains personnel in their incident response roles and responsibilities with respect to the information system and provides refresher training on a defined frequency.
	Organization implements an incident handling capability for security incidents.
	Organization tracks and documents information system security incidents.
	<i>Hardware and System Software Maintenance</i>
	A formal, documented information system maintenance policy exists and is implemented.
	Access is limited to system software and hardware.
	Organization schedules, performs, documents, and reviews records of maintenance (controlled maintenance) and repairs on information system components in accordance with manufacturer or vendor specifications and/or organizational requirements; controls all maintenance activities (on-site or remote).
	Organization approves controls, monitors the use of and maintains information system maintenance tools.
	Organization obtains maintenance support and/or spare parts for a defined list of security-critical information system components and/or key information technology components within a defined time period of failure.
	All new and revised hardware and software is authorized, tested, and approved before implementation
	Software change request forms are used to document requests and related approvals
	Controls are adequate to restrict access to the database and database utilities
	The type of test data to be used is specified, i.e., live or made up
	Software distribution implementation orders including effective date provided to all locations exist
	Version control is implemented
	Contingency plans and other associated documentation are updated to reflect system changes
	Systems are periodically reviewed to identify and, when possible, eliminate unnecessary services (e.g., FTP, HTTP, mainframe calls)
	<i>Data Integrity</i>
	Virus detection and elimination software is installed and activated.
	Firewalls and/or proxy servers used and their software are described
	The level of data encryption used, if any, and whether it is hardware or software-based is described

	The application languages being used (HTML, XML, JavaScript, etc.) and whether they are static, semi-dynamic, or dynamic is described
	Database connectivity and any APIs being used is described
	Hardware and software, if using separate web servers, is described
	The controls in place for shared resources including any of the following are described: <ul style="list-style-type: none"> I. Password protection II. User groups III. Smartcards IV. Biometrics V. Virus Scanners VI. Vulnerability scanners VII. Intelligent agents
	Data integrity and validation controls are used to provide assurance that the information has not been altered and the system functions as intended
	Inappropriate or unusual activity is reported, investigated, and appropriate actions taken
	Procedures are in place to determine compliance with password policies
	Intrusion detection tools are installed on the system
	Penetration testing is performed on the system
	Message authentication is used
	All system and data accesses are logged
	<i>Documentation</i>
	There is sufficient documentation that explains how software/hardware is to be used.
	There is application documentation for in-house applications
	There are network diagrams and documentation on setups of routers and switches
	Software and/or documentation is properly logged, checked out, and locatable at all times
	There are software and hardware testing procedures and results
	There are user manuals
	There are backup procedures
	<i>Security Awareness, Training, and Education</i>
	Employees receive adequate training to fulfill their security requirements.
	There is mandatory annual refresher training
	<i>Incident Response Capability</i>
	The capability exists to provide help to users when a security incident occurs in the system.
	Incidents are monitored and tracked until resolved
	Personnel are trained to recognize and handle incidents
	Incident information and common vulnerabilities or threats is shared with owners of interconnected systems
TECHNICAL CONTROLS	
Focus on controls the computer system executes. The controls can provide automated protection for unauthorized access or misuse, facilitate detection of security violations, and support security requirements for applications and data. These controls should be consistent with the defined security management of the State or agency.	

<i>Identification and Authentication</i>	
	Organization develops, disseminates, and reviews/updates on a defined frequency a formal, documented identification and authentication policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and formal procedures to facilitate the implementation of the policy and associated controls.
	The information system uniquely identifies and authenticates organizational users (or processes acting on behalf of users).
	The organization manages information system identifiers for users and devices by receiving authorization from a designated organizational official to assign a user or device identifier, selecting an identifier that uniquely identifies an individual or device, assigning the user identifier to the intended party or device; preventing reuse of user or device identifiers and disabling user identifiers after a defined period of inactivity.
	The information system obscures feedback of authentication information during the authentication process to protect the information from possible exploitation/use by unauthorized individuals.
	The information system uniquely identifies and authenticates non-organizational users (or processes acting on behalf of non-organizational users).
	Users are individually authenticated via passwords, tokens, or other devices.
	Emergency and temporary access may be authorized
	Personnel files are matched with user accounts to ensure that terminated or transferred individuals do not retain system access
	Passwords are changed at least every 90 days. (state # of days)
	Passwords are unique and difficult to guess (alpha/numeric, special characters). (provide password schema)
	Inactive user IDs are disabled after a specified period of time
	Passwords are distributed securely and users informed not to reveal their passwords to anyone (social engineering)
	Vendor-supplied passwords are replaced immediately
	There is a limit to the number of invalid access attempts that may occur for a given user. (state limit)
	Access controls enforce segregation of duties
	Data owners periodically review access authorizations to determine whether they remain appropriate
	Are user logons/passwords challenged frequently and under a multi-level protection scheme?
	Do you allow synchronization of passwords for single sign-on?
	Describe the number of staff that have administrative rights to the application, telecomm, and web servers and how access rights are separated
	User profiles/roles and permissions protocol to be used are described.
	The system uniquely identifies and authenticates a defined list of specific and/or types of devices before establishing a connection.
<i>Logical Access Controls</i>	

	Communication protocols being used (FTP, HTTP, Telnet, etc.) are described
	Access controls are described. <ul style="list-style-type: none"> I. Identification and authorization II. Sensitive and privacy III. No repudiation IV. Data integrity
	How the organization develops, disseminates, reviews/updates a formal, documented access control policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance is described.
	How the organization manages information system accounts is described, including: identifying account types (i.e., individual, group, system, application, guest/anonymous, and temporary)
	How logical access controls restrict users to authorized transactions and functions is described.
	Separation of Duties of individuals as necessary to prevent malevolent activity without collusion; document separation of duties, and implements separation of duties through assigned system access authorizations.
	The organization employs the concept of least privilege, allowing only authorized accesses for users (and processes acting on behalf of users) which are necessary to accomplish assigned tasks in accordance with organizational missions and business functions.
	The information system enforces a limit of consecutive invalid access attempts by a user during a defined period.
	The information system displays an approved system use notification message or banner before granting access to the system that provides privacy and security notices consistent with applicable laws.
	Access to security software is restricted to security administrators.
	The information system limits the number of concurrent sessions for each system account to a defined number.
	How workstations disconnect or screen savers lock system after a specific period of inactivity or upon receiving a request from a user; and retains the session lock until the user reestablishes access using established identification and authentication is described.
	Any encryption used and what type is used.
	Access is restricted to files at the logical view or field.
	Logical controls over network access are described.
	Controls that restrict remote access to the system are described.
	If the network connection automatically disconnects at the end of a session is described.
	Firewalls or secured gateways installed are described.
	If the public accesses the system, controls implemented to protect the integrity of the application and the confidence of the public are described.
	A privacy policy posted on the web site.
	The organization documents allowed methods of remote access to the information system; establishes usage restrictions and implementation guidance for each allowed

	method; monitors for unauthorized remote access; authorizes remote access prior to connection; and enforces requirements for remote connections.
	The organization establishes usage restrictions and implementation guidance for wireless devices and for organization-controlled mobile devices; authorizes connection; monitors for unauthorized access; and enforces organizational policies and procedures.
	The organization establishes terms and conditions, consistent with any trust relationships established with other organizations owning, operating, and/or maintaining external information systems, allowing authorized individuals to access the information system from external information systems; and process, store and/or transmit organization-controlled information using external information systems.
	<i>Audit Trails and Accountability</i>
	Activity involving access to and modification of sensitive or critical files logged, monitored, and possible security violations investigated.
	Off-line storage of audit logs is retained for a period of time. How access to these logs is strictly controlled is described.
	Organization develops, disseminates, and reviews/updates on a defined frequency a formal, documented audit and accountability policy that addresses purpose, scope, roles, responsibilities, and management commitment, coordination among organizational entities, and compliance; and formal documented procedures to facilitate the implementation of audit and accountability policy and associated audit controls.
	Organization determines, based on a risk assessment and mission/business needs, the system must be capable of auditing a defined list of auditable events; coordinates the security audit function with other organizational entities; and based on current threat information and ongoing risk assessment that the events are to be audited within the information system.
	Produces audit records that contain sufficient information, at a minimum, to establish what type of event occurred, when (date and time) the event occurred, where, the source of the event, and the outcome (success or failure), and the identity of any user/subject associated with the event.
	The information system provides an audit reduction and report generation capability.
	The information system uses internal system clocks to generate time stamps for audit records.
	The information system protects against an individual falsely denying having performed a particular action (non-repudiation).
	Audit records are retained for a defined period of time consistent with records retention policy to provide support for after-the-fact investigations of security incidents and to meet regulatory and organizational information retention requirements.
	The organization monitors open source information for evidence of unauthorized ex-filtration or disclosure of organizational information on a defined frequency.
	The information system provides the capability to capture/record and log all content related to a user session; and remote hear/view all content related to an established user session in real time.
	<i>System and Communications Protection</i>
	Organization develops, disseminates, and reviews/updates on a defined frequency a

	formal system and communications protection policy that addresses purpose, scope, roles, responsibilities, coordination among organizational entities, and compliance.
	Information system separates user functionality (including user interface services) from information system management functionality.
	Information system isolates security functions from non-security functions.
	Information system prevents unauthorized and unintended information transfer via shared system resources.
	Information system prevents against or limits the effects of a defined list of denial of service attacks.
	Information system limits the use of resources by priority.
	Information system monitors and controls communications at the external boundary of the system and at key internal boundaries within the system; and connects to external networks or information systems only through managed interfaces consistent of boundary protection devices arranged in accordance with organizational security architecture.
	Information system protects the integrity of transmitted information.
	Information system terminates the network connection associated with a communications session at the end of the session or after a defined period of activity.
	Information system protects the confidentiality of transmitted information.
	Information system establishes a trusted communications path between the user and the defined security functions of the system to include at a minimum, information system authentication and reauthentication.
	Information system protects the integrity and availability of publicly available information and applications.
	Information system prohibits remote activation of collaborative computing devices with a list of defined exceptions where remote activation is to be allowed; and provides an explicit indication of use to users physically present at the devices.
	Information system associates security attributes with information exchanged between information systems.
	Organization defines acceptable and unacceptable mobile code and technologies, establishes restrictions and implementation guidance for acceptable code and technologies, and authorizes, monitors, and controls the use of mobile code within the information system.
	Organization establishes usage restrictions and implementation guidance by Voice over Internet Protocol (VoIP) technologies based on the potential to cause damage to the information system if used maliciously; and authorizes, monitors, and controls the use of VoIP within the information system.
	Information system provides additional data origin and integrity artifacts along with the authoritative data the system returns in response to name/address resolution queries.
	Information system performs data origin authentication and data integrity verification on the name/address resolution responses the system receives from authoritative sources when requested by client systems (recursive or caching resolver).
	Information systems that collectively provide name/address resolution service for an organization are fault-tolerant and implement internal/external role separation.

	Information system fails to a defined known-state for defined types of failures preserving defined system state information in failure.
	Organization partitions the information system into components residing in separate physical domains (or environments) as deemed necessary.
	Information system loads and executes the operating environment from hardware-enforced, read-only media; and loads and executes defined applications from hardware-enforced, read-only media. (non-modifiable executable programs)