Department of Health and Human Services

Information Security Manual

Prepared by the Privacy and Security Office

Table of Contents

CHAPTER 1: INTRODUCTION TO THE INFORMATION SECURITY PROGRAM

1.1 Purpose

Divisions and Offices (see below) are becoming more dependent on information technology (i.e., systems) and the data contained within to successfully carry out their essential functions and business services. Systems (see below) can include as constituents a broad range of technologies (e.g. individual components; network and telecommunication systems; computers; tablet; smart phones; etc.) and services. DHHS faces an ever-changing threat-landscape that can have adverse impacts on Department operations (e.g. essential functions, business services, regulatory compliance, reputation, and financial), Department assets, individuals, partner Divisions and Offices, and the State by compromising the confidentiality, integrity, or availability of data entrusted to DHHS and being processed, stored, or transmitted by Department systems. Threats to data and systems include environmental disruptions, human or machine errors, and purposeful attacks (e.g. cyber-attacks which are often aggressive, disciplined, well organized, well-funded, and in a growing number of documented cases, very sophisticated). Given the significant and growing danger of these threats, it is imperative that all levels of the organization understand their responsibilities for achieving adequate data security and for managing system-related security risks.

The term organization is used in this manual to describe an entity of any size, complexity, or positioning within the DHHS Department structure (e.g. divisions, offices or as appropriate, any of the department's operational elements).

A system is a discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of data used or operated by an organization, a contractor of an organization, or by a third-party on behalf of a DHHS organization.

1.2 Approach

This manual is designed to be a baseline for the application of a risk-based approach (see Chapter 6: Risk Management) to protecting Department data and systems and based on the principle that the right to data protection is a qualified right. Because of this it is not designed to function as a standalone document or intended to be the de facto security rule; but rather it is to be used in conjunction with the Statewide Information Security Manual and enhanced through the creation of organization-specific standards, policies, and processes as required.

This manual does not override any Department obligations imposed by legislation or law. Furthermore, if this manual conflicts with legislation or law the later takes precedence.

1.2.1 Alignment with the Statewide Information Security Manual

The Statewide Information Security Manual wis based off of the NIST 800-53 R4 framework and serves as the foundation for information technology security in North Carolina. Specific requirements, practices and recommendations contained within the Statewide Information Security Manual are not repeated within this manual unless required for clarity of material.

1.2.2 Alignment with the Framework for Improving Critical Infrastructure Cybersecurity

In February 2013, the Office of the President issued the Executive Order on "Improving Critical Infrastructure Cybersecurity ". The Framework gathers existing global standards and practices to help Divisions and Offices understand, communicate, and manage their cyber risks. The risk based approach of the DHHS Information Security Manual coupled with the State foundational framework is designed to align with our responsibilities in regards to Critical Infrastructure Cybersecurity.

1.2.3 Alignment with Information Security Best Practices

Building upon the foundation laid by the Statewide Information Security Manual, DHHS has chosen to adopt best practice standards as detailed by the National Institute of Standards and Technology (NIST) to provide security enhancements and guidance to Department data and systems.

1.2.4 Maintenance, Reviews and Updates

NC DHHS Security Manual reviews and updates shall be conducted on an annual basis. New policies shall be reviewed by the DHHS Privacy and Security Office and routed to authorized personnel for approvals. Material revisions shall be reviewed and approved at

the discretion of authorized personnel. Policies shall be approved prior to publishing to make accessible for all Divisions and Offices. All approved policies shall be provided to Divisions and Offices to include documentation of review dates, update dates, and approval dates for maintenance. NC Divisions and Offices shall maintain their program specific policies and procedures and ensure they align with DHHS Security Manual where applicable to include annual review, updates, and documentation of approval and enforcement.

Updates to the Statewide Information Security Manual shall be reviewed annually and as made available by the North Carolina Division of Information Technology. Updates to the Statewide Information Security Manual shall be reviewed annually and adopted within 90 days where there are more restrictive implementation requirements that impact NC DHHS Offices and Divisions. Version control numbers will be assigned based on type of revision as minor or major. Minor revisions will show version control number (vX_XX), major revisions will show v(XX). "v" shall mean version and "XX" indicates the number.

1.3 Applicability

Unless denoted by applicability all sections and subsections of this manual are required by all Divisions and Offices. Additionally, all devices, equipment and systems accessing Department data must meet statewide, departmental and applicable federal security controls or have appropriate mitigations. Control mitigations requirement compliance must be documented.

Divisions and Offices shall develop a policy and procedure where there are program specific federal requirements as applicable and are not less restrictive than this policy manual, Statewide Information Security Manual, and other state or federal requirements. Contracts with vendors shall reflect the grace period of 90 days to implement applicable change and addendums into the contract language.

-- Remainder of Page Intentionally Left Blank --

CHAPTER 2: PERSONNEL SECURITY

2.1 Pre-Employment Screening

Divisions and Offices must follow DHHS Division of Human Resources and the Office of State Human Resources policies and procedures for the conducting of pre-employment screenings. Pre-employment screening includes but is not limited to; reference checks, criminal history checks, educational verification, license verification, and sanctions checks.

2.2 Documentation of Job Descriptions

In accordance with the DHHS Division of Human Resources and the Office of State Human Resources, Divisions and Offices shall create, document, and monitor their workforces' job descriptions. Job descriptions must clearly and accurately define all roles and responsibilities for all job functions including but not limited to duties, responsibilities, required qualifications, reporting structure (i.e. manager's title, dotted line reporting relationships, etc.) and types of data to be accessed (i.e. Health Insurance Portability and Accountability Act (HIPAA), Internal Revenue Service (IRS), Social Security Administration (SSA), etc.)

Workforce job descriptions shall be used during the process of determining training requirements, business need identification, and for ensuring workforce members are assigned appropriate levels of access rights. Workforce member must be provided with a copy of their job description when they are informed of the access granted to them, and the conditions by which this access can be used.

Guidelines

In an effort to avoid missing key functions, job descriptions must be developed in cooperation with Department Human Resources (HR) officers but written by individuals with first-hand knowledge of job requirements and inner workings. Accurate and well thought out job descriptions can not only be used as part of a performance management process but serve as a foundation for the separation of duties.

2.2.1 Separation of Duties and Least Privilege Requirements

Divisions and Offices shall ensure that workforce members' roles and responsibilities are based on separation of duties and least privileges to ensure that security access levels are appropriately distributed.

Workforce members are required to segregate access between users who have access to confidential information and those who do not. Divisions and Offices must also ensure that appropriate controls for access extend between themselves and their outsourced functions.

Guidelines

Documented reporting structures identifying to whom and for what purpose individuals report should be used to assist in evaluation for appropriate accountability, and aid in implementing separation of duties and least privilege. As part of the reporting structure review individual's Independence of Operation (i.e. the authority for individuals to make decisions and the way in which they are referred upwards for action/approval), and the extent of supervision required (e.g. work is fully-checked, spot-checked or generally review, etc.) should be looked at including the potential impact of decisions, actions and recommendations.

2.3 Workforce Authorization and Clearance

All Department workforce members must comply with required federal, state and department regulations. When employing or contracting new workforce members, Divisions and Offices must ensure that each new workforce member completes any required security, privacy or regulatory training prior to allowing access to confidential data.

2.3.1 Third-Party Contractors

In order to perform the requested services, a third-party contractor may need to utilize departmental information resources and/or access confidential information. In these instances, Divisions and Offices must ensure that access granted is the minimum necessary required for performing roles and responsibilities. The appropriate Data Steward must approve and have full knowledge of the access rights obtained by the third-party contractors.

Data and information belonging to the department must not be released to third-party contractors without proper documented agreements, specifying the conditions of use and security requirements in place, between the third-parties and organization management. These documents may include but are not limited to non-disclosure agreements (NDA), business associate agreements (BAA) and service level agreements (SLA).

Third-party contractors should be fully contractually accountable to the organization for any actions taken while completing their roles and responsibilities. Divisions and Offices must ensure that applicable federal, state and departmental regulations are communicated to third-party contractors.

Guidelines

Divisions and Offices shall develop and implement procedures for the determination and authorization of all (e.g. third-parties, business associates, vetted employees, contractors, etc.) who have access to federal, state, departmental networks, information or data.

2.4 Workforce Disciplinary Actions

Divisions and Offices shall develop policies and procedures for appropriately applying sanctions (e.g. reprimand, termination) against workforce members that fail to comply with required security regulations.

All sanctions must conform to the policies, procedures, standards, and guidelines handed down by the DHHS Division of Human Resources, and the Office of State Human Resources. In addition, all DHHS workforce members with potential access to Electronic Protected Health Information (ePHI) must have a signed copy of the "Understanding of DHHS HIPAA Sanctions".

2.5 Separation of Service Requirements

A separation of service occurs but is not limited to when the DHHS workforce member resigns, retires, is dismissed/terminated, selected for reduction in force (RIF) or transfers to a state agency external to DHHS. Divisions and Offices shall develop policies and procedures for appropriately handling workforce separation of service.

2.5.1 Termination of Employment

Divisions and Offices must implement procedures to ensure that when a workforce member's employment terminates:

- All system accounts are terminated
- All access to departmental information/data is removed
- All access to facilities, including but not limited to card access, keys, codes, and other facility access control mechanisms is terminated
- Workforce Identification (ID) Badge is collected
- Work related keys including, but not limited to, office door keys, desk keys, file drawer or cabinet keys, etc., are turned in
- Codes or passwords for systems, equipment access passwords (firewalls, routers, etc.), administrator passwords, and other common access control information should be changed when appropriate
- The Division of Human Resources is promptly notified

2.5.2 Transfer of Employment

If a workforce member transfers to another organization within DHHS the workforce member's access must be terminated as of the date of transfer. The workforce member's new organization is responsible for establishing all required access for the workforce member's new role and responsibilities.

2.5.3 Temporary Separation of Service

In some instances, as deemed necessary by Divisions and Offices, workforce members who are on extended leave for more than four (4) weeks or twenty (20) working days may be required to have temporary security constraints placed on their access to organization systems and facilities. These constraints must be defined and documented within the organization's "Termination of Employment Procedures" as required by section 2.5.1. Extended leaves of absence include but are not limited to medical, investigative, administrative and annual leave; suspension; sabbaticals or extended leave without pay.

2.6 Handling Personnel Information

DHHS workforce members and others are prohibited from seeking out, using, or disclosing personal information collected during the pre-employment screening, employment, disciplinary and termination process(s) except within the scope of their assigned duties or as permitted by the DHHS Division of Human Resources and the Office of State Human Resources.

2.7 Information Security Education Training and Awareness (SETA)

Security education, training and awareness are not alternatives to technological security controls but rather complementary and mutually supportive approaches that focus on roles and responsibilities specific to individuals.

Divisions and Offices are responsible for developing SETA programs specific to their business, and for ensuring all workforce members know their responsibilities related to required security training and awareness courses.

Workforce security awareness and training shall at a minimum include, but not be limited to:

- Reading the "Acceptable Use for DHHS Resources"
- Legal responsibilities associated with regulatory compliance (e.g. copyright, software, intellectual property, HIPAA, IRS, SSA)
- Annual, general information security training (e.g. how to report incidents, roles and responsibilities reacted to information security, password management, etc.)
- Sign the "Acceptable Use for DHHS Resources" policy

In addition, Divisions and Offices as part of their SETA program shall provide periodic security updates to workforce, third-party contractors and where appropriate external business associates.

2.7.1 Developing a Security Education Training and Awareness Program

SETA programs must be designed in alignment with the organization's mission and support its business needs. SETA efforts must be formally documented, and Department endorsed.

During the development phase of the program, the organization's training and awareness needs are identified, an effective training and awareness strategy is realized, Department buy-in is sought and secured, priorities are established, and materials developed.

Conduct A Needs Assessment

Divisions and Offices must conduct needs assessments in order to define criteria for SETA efforts.

A properly conducted needs assessment will allow Divisions and Offices to explore what skills/knowledge workforce members have, what they need, and then make an informed estimate of the changes required to successfully address any identified gaps. When conducting a needs assessment, it is important that key personnel be identified and involved.

Guidelines

Divisions and Offices should use a variety of sources for information gathering during the needs assessment. Different techniques in which information can be gathered as part of a needs assessment include but are not limited to:

- Interviews or conversations with identified key groups/workforce members
- Department surveys
- Review of available resource material and metrics related to current awareness and training efforts
- Review of findings/recommendations from oversight bodies or program reviews
- Analysis of events, such as social engineer attempts, that might indicate the need for training or additional enhancements to current training
- Conduct trending analyses to provide insight into possible unidentified issues
- Review current and forthcoming regulatory requirements

- Direct observation and work analyses

NIST Special Publication 800-50 (Building an Information Technology Security Awareness and Training Program) contains a sample needs assessment interview and questionnaire.

Developing a Strategy

Information from the completed needs assessment shall be used by Divisions and Offices to develop a realistic strategy (working plan) for prioritizing, budgeting, creating, implementing, and maintaining their SETA efforts. The plan should identify and outline the following elements:

- Scope with long and short-term goals
- Target audience, required knowledge level and frequency of exposure to material
- Topics with learning objectives
- Roles and responsibilities of organization personnel related to plan elements
- Material and resource requirements
- Deployment methods
- Evaluation, feedback, and metrics
- Estimated funding requirements

Establishing of Priorities

Divisions and Offices should prioritize training and awareness efforts based on the documented plan elements, the effort's Department impact, current state of compliance, and project dependencies.

Developing Materials

Prior to developing any materials, Divisions and Offices must determine whether they are developing awareness or training materials, or a combination thereof. Typically, awareness materials are short and simple messages focusing generally on high-level practices, whereas training materials are in-depth, and directed at a specific audience.

SETA materials should be designed to fit within budgetary allowances and to incorporate back into DHHS workforce jobs to address current Department missions, business, technology, and data security requirements. Materials designed should facilitate results based learning, and be considerate of various learning styles, i.e., visual, auditory or tactile.

Materials can be developed using one theme (topic) at a time or created by combining a number of themes into a campaign.

Sources for materials can come from a variety of places such as professional Divisions and Offices, websites, periodicals, conferences, seminars, vendors, etc. Sources selected for use in developing SETA programs should be current and should provide a feeling that the material was developed specifically for the intended workforce members.

Guidelines

Divisions and Offices should consider the following questions when developing program materials:

- "What behavior(s) do we want to reinforce?"
- "What skill(s) do we want the audience to learn and apply?"

Individuals developing courses and materials should be aware that adults have established, not formative, values, beliefs, and opinions as it relates to education and training; learning style preferences will differ based on education, years of experience, and previous learning experiences. Materials should be designed to present new material while at the same time allow for the sharing of relevant experiences. Instructors can help to make connections between various student opinions and ideas, while focusing class effort on integration of the new knowledge or skill with respect to its application.

Designing Metrics

Metrics are an important and effective tool that can be used to demonstrate compliance, gauge program effectiveness and provide quantifiable information for decision making processes.

Metrics are expressed using at least one (1) unit of measurement and should be:

- **Transparent:** Simple and easy to understand, common interpretation
- **Meaningful:** Relevant to business processes or objectives, contextually specific
- **Actionable:** Able to influence work
- **Accessible:** Come from creditable data sources, cheap to gather
- **Repeatable:** Little or no subjectivity, consistently measured

Guidelines

SETA programs at a minimum should compile and track:

- **Implementation metrics:**
    - Demonstrate progress in implementing the program's specific required processes or controls
    - Data should be numerical and easily obtained from various reports, plans of action or other commonly used means of documenting and tracking program activities (e.g. percentage of employees who have completed training)
- **Impact metrics:**
    - Organization-specific measures that combine information about the results of the programs implementation with a variety of information about resources
    - Tracking a variety of resource information across the organization in a manner that can be directly tied to program activities and events

2.7.2 Delivering SETA to Workforce Members

Many techniques exist to deliver SETA messages throughout an organization. The organization's chosen technique(s) should be identified and documented within the working plan 2.7.1 Developing a Security Training and Awareness Program and be chosen based upon available resources, budgeting and the complexity of the message(s) to be conveyed at the time.

Techniques for effectively delivering training materials should be evaluated for:

- Ease of use (e.g. easy to access and easy to update/maintain)
- Scalability (e.g. can be used for various audience sizes and in various locations)
- Accountability (e.g. capture and use statistics on degree of completion)
- Broad support base (e.g. adequate number of potential vendors, better chance of finding follow-on support)

Guidelines

Organization information security awareness communication methods may include, but not be limited to the following:

- Electronic methods such as emails, screen savers, pop-up messages, digital newsletters, web or teleconference sessions and other media depending on the complexity of the information security awareness messages
- Physical methods such as pamphlets, posters, "Brown bag" seminars, instructor-led sessions, messages on used tools (e.g. flash drives, pens, notepads)
- An annually updated workforce member handbook that contains information security awareness policies, requirements and safeguards. It is recommended that Divisions and Offices choosing to create a workforce member handbook formally deliver the material to workforce members within the first sixty (60) days of employment and require individuals to sign a statement of understanding before allowing workforce members access to departmental data.

2.7.3 Program Evaluation and Feedback

Security training and awareness efforts, including program strategies, must be reviewed annually, or as required by regulation, to ensure they continue to meet requirements. The scope of the review must include, but not be limited to the following:

- Introduction of new technologies and associated risks
- Updates to data regulations (e.g. HIPAA, IRS 1075, SSA)
- Input from workforce members concerning the effectiveness of SETA programs
- Evaluation of training and awareness metrics

Guidelines

Program evaluation and feedback information should be anonymously recorded to allow for honest options. Formal evaluation and feedback mechanisms (e.g. evaluation forms/questionnaires, independent analysis, etc.) are critical components of any training and awareness program as programs should strive for continuous improvement. Evaluation and feedback mechanisms must be designed with elements that will address quality, scope, deployment method, level of difficulty, ease of use, duration of session, relevancy, currency, and suggestions for modification.

Evaluation and feedback data should be aggregated at both the individual course and program level allowing for the identification of areas that require improvement at both levels.

Identified areas of improvement should be evaluated, prioritized and documented with associated program improvements within a Corrective Action Plan (CAP). Items documented within the CAP should be included in future budgeting considerations and program cost-benefit analysis.

2.7.4 Professional Development and Education

Professional development is intended to ensure that users possess a required level of knowledge and competence necessary for their roles. Professional skills are often validated through either certification or education.

Guidelines

DHHS workforce members are encouraged to improve their professional knowledge, skills, qualifications, and experience by:

- Obtaining membership in professional Divisions and Offices, boards, or focus groups
- Receiving subscriptions to technical documents (e.g., newsletters, magazines, and white papers)
- Obtaining certifications relevant to information security
- Attending a higher education institution

2.7.5 Training Documentation

Up-to-date documentation of completed professional development, education, awareness and training activities should be retained within individual workforce members' personnel files. Documentation shall be retained in accordance with NC Department of Cultural Resources (DCR) - Government Records Branch of NC or as required by regulation.

2.8 Personnel Safety

Divisions and Offices must assess personal safety risks (e.g. working alone, work-related violence, etc.) as part of a comprehensive Risk Management process (see Chapter 6: Risk Management).

-- Remainder of Page Intentionally Left Blank –

CHAPTER 3: DATA LIFECYCLE MANAGEMENT

3.1 Data Ownership

For the purposes of determining data roles and responsibilities DHHS has adopted a federated data-related accountability approach. Under this method DHHS will serve as the "Data Owner" for all departmental data.

As a Department data owner, DHHS delegates accountability and stewardship through data-based roles and responsibilities to Divisions and Offices under its departmental umbrella.

3.1.1 Criteria of Ownership

Data is defined to be owned by DHHS if it meets any of the following criteria:

- The data is created specifically by or for DHHS
- The data is collected specifically for use by DHHS
- The department is given ownership through statutory or regulatory requirement(s)
- The department is given specific ownership through a written agreement

3.2 Data Classification, Naming and Labeling

For the purposes of this manual the term data includes information (i.e., processed data) and data in all its forms regardless of location, media or characteristics.

3.2.1 Data Classification

Divisions and Offices shall explicitly classify data as confidential or public. Data classification is to be determined in accordance with NC General Statutes (G.S.) Chapter 132 Public Records Law and all other applicable legal or regulatory requirements. The data must be given the same classification regardless of the storage medium (e.g. paper, tape, optical media, portable flash memory drives, electronic file, etc.).

Public Data (e.g. meeting agendas and minutes, job postings, information on departmental websites, etc.):

- Is created in the normal course of business that is unlikely to cause harm
- Has no regulatory restrictions related to access, storage or usage
- Limited safeguards related to access, storage or usage
- Open to public record requests
- Unrestricted access (i.e., information is available to citizens, DHHS workforce and third parties)
- No special handling required
- Can be recycled
- Minimal impact if lost, changed or denied access

Confidential Data (e.g. social security numbers, Personally Identifiable Information (PII), credit card numbers, medical records, Federal Tax Information (FTI), etc.):

- Is limited to authorized users with a demonstrated and documented need-to-know
- Has regulatory restrictions or safeguards related to access, storage or usage
- Must not be posted on any public website
- May not be disclosed without explicit authorization
- Stored with appropriate physical and logical access controls
- Requires protection during transmission
- Must be destroyed when no longer needed
- Requires sanitization prior to equipment disposal, reuse or being serviced by an external/third-party
- The loss, damage or unavailability causes an increased impact such as loss of opportunity, loss of organization/program confidence on behalf of the citizens, or financial or regulatory sanctions

Guidelines

Personally Identifiable Information refers to information which can be used to distinguish or trace an individual's identity, such as their name, social security number (including last four (4) digits), biometric records, etc. alone, or when combined with other personal or identifying information which is linked or linkable to a specific individual, such as date and place of birth, mother's maiden name, etc.

PII also includes any information that could be used to reference other data elements that are used for identification, such as gender, race, and date of birth.[1]

This definition of PII is not anchored to any single category of data or technology. Rather, it requires a case-by-case assessment of the specific risk that an individual can be identified. When performing this assessment, it is important to recognize that 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.[2]

The US Department of Commerce and NIST publication 800-122 titled "Guide to Protecting the Confidentiality of Personally Identifiable Information (PII)" provide additional guidance related to the identification and protection of PII.

3.2.2 Data Naming

To facilitate data sharing, reduce complexity and confusion from data elements made or received in connection with the transaction of business by DHHS, Divisions and Offices shall develop a standardized naming convention along with an inventory of data elements.

Guidelines

Data naming conventions should be easy to follow and allow for the creation of applications that do not introduce ambiguity or misunderstanding during the phases of the System Development Life Cycle (SDLC), agreements or in connection with departmental data exchanges. When developing a data naming convention, considerations should be given but not limited to character limits, response times, storage, maintenance and business requirements, and application or computing environment limitations.

Data inventories must be periodically reviewed and updated to ensure comprehensiveness.

3.2.3 Data Analysis Protection

Data analysis can be used to efficiently discover, parse and analyze valuable (i.e., useful) information from large amounts of data. Outputs from the varied analysis techniques can be used to create conclusions and support business decision making.

Divisions and Offices must ensure that procedures and safeguards are in place to prevent the use of data analysis techniques such as data mining (i.e., modeling and knowledge discovery for predictive purposes) to harvest or discover confidential departmental data from systems, including those that do not directly contain confidential information.

Guidelines

Where possible, unique identification numbers should be substituted for confidential data during data analysis processes in an effort to prevent both accidental and intentional data loss. Identification numbers for identical data fields (e.g. last name, address, prescription code, etc.) should allow for cross system data (i.e., identical data stored in multiple systems) to be analyzed together.

3.2.4 Data Labeling

Divisions and Offices shall explicitly label all data classified as confidential regardless of form or media.

Guidelines

[1] Taken from U.S. Department of Commerce Office of the Chief Information Officer (http://ocio.os.doc.gov/ITPolicyandPrograms/IT_Privacy/PROD01_008240)
[2] Taken from the General Services Administration Rules and Policies - Protecting PII - Privacy Act (http://www.gsa.gov/portal/content/104256)

Physical (e.g. printed documents, reports, handouts, faxes) containing confidential data must have a clearly visible confidential label on every page; folders and coversheets for confidential documents must also carry a confidential label. Digital media (e.g. slides, electronic documents) containing confidential data must display a clearly visible confidential label, and where possible contain a confidential data label within the file's metadata. Systems (e.g. servers, network storage) containing confidential data must display warning banners identifying the data contained within as confidential. Confidential data that is verbally disclosed should be orally identified as confidential prior to initiation of the discussion; parties/individuals involved in the discussion may be required to sign/receive written notice as to the confidentiality of the data.

3.3 Roles and Responsibilities Related to Data Management

The following roles and responsibilities must be identified to ensure that organization data is secured, safeguarded, and handled appropriately:

- **Data Steward (Business):** Represent the data owner, when data is being discussed in reference to its distribution, alteration, storage, retention, disposition or classification, focus on managing data content and the business logic, provide advice for protection and operational management of data, act as the point-of-contact or liaison who will oversee the implementation and performance of activities associated with the managing or implementation of data resources.

- **Data Custodian (Technical):** Oversee the safe transport, storage and disposition of data with an underlying focus on the infrastructure, activities and safeguards required to maintain the confidentiality, integrity and availability of the data. Collaborate with the Data Stewards in the implementation of data transformations, resolution of data issues, and collaborate on system changes. Act as the point-of-contact or liaison, which will oversee the implementation of data protections and provide an understanding on the reporting of security risks and how they impact the confidentiality, integrity and availability of Department data.

- **System Administrator:** Department workforce members who are responsible for provisioning, de-provisioning, and auditing access to departmental data as authorized by the Data Steward; aid in ensuring that adequate safeguards are implemented and documented. Act as a representation of the user community in the provisioning and selection of information resources. The System Administrators shall ensure correct authorization and account management processes and procedures are followed for their specific system. A System Administrator shall maintain, enable, and disable workforce members' access levels to a particular body (i.e., system or system component) of Department data.

- **Data User:** A data user is a workforce member who has been provisioned by a System Administrator to perform required roles and responsibilities. The data users shall not be allowed to alter or delete data contained within a body, unless the approved Data Stewards/System Administrator has granted them the permission and rights to do so. Data Users are responsible to understand data requirements, assist in the data control function, and work with System Administrators to share information about applications and technologies (i.e., what works and what does not).

3.3.1 Recording Roles and Responsibilities

Divisions and Offices shall be responsible for creating and maintaining documentation of data responsibilities including but not limited to: lists of all Data Stewards, Data Custodians and System Owners that have authorization and access controls to DHHS data. The Division ISO shall be responsible for monitoring their organization's records periodically to ensure that changes are updated accordingly.

Guidelines

Divisions and Offices, with the assistance from identified Privacy and Security Officials, shall determine the data roles and responsibilities, prior to posting job qualifications; all appropriate duties shall be included in the job vacancy list. In addition, Divisions and Offices must notify Data Stewards, Data Custodians, and System Owners when duties change to ensure job roles and responsibilities are carried out appropriately.

3.4 Data Flow Diagram Development

A Data Flow Diagram (DFD) is a high-level graphical representation of how data logically flows through a system's components, boundaries, external entities and other connected systems. The DFD shows how entities (i.e., data inputs/source and

outputs/destinations), processes (i.e., how the data is manipulated or used), data stores (i.e., where data will be stored at rest while waiting to be used by a process), and data flows (i.e., the movement of data between the entity, process, and data store) are logically related.

The DFD is not expected to show information about data process timing or whether they operate in sequence or in parallel.

Guidelines

Divisions and Offices shall create DFDs for each of their systems. The level of detail and complexity to the DFD is at the sole discretion of the division and office as long as the diagram meets the minimum requirements set forth in 3.4 Data Flow Diagram Development above.

DFDs can be used to assist in the assigning of appropriate data-related accountability to Data Stewards, Data Custodians, System Owners and Data Users.

3.5 Data Access

Divisions and Offices shall ensure that data is readily available to appropriate DHHS workforce members except when access restrictions have been determined appropriate and applicable.

Guidelines

Divisions and Offices must create, enforce and monitor procedures and processes that ensure all members of their workforce have appropriate access to information, as required to carry out their assigned duties, and to prevent non-authorized individuals from obtaining DHHS data. Also when utilizing, disclosing or requesting confidential information, Divisions and Offices must make reasonable efforts to limit information to the minimum necessary to accomplish the intended purpose of the use, disclosure or request.

3.6 Records Management

Records including but not limited to: documents, files, reports, data requests and logs must be managed, retained, archived and organized in such a way that they are retrievable in a coherent format (i.e., easily understandable). At a minimum Divisions and Offices must ensure records are:

- Maintained with appropriate security controls (e.g. encryption) in place based on the records data;
- Verified after the transfer between formats or in preparation for archival to ensure the integrity of the records data;
- Retained or archived as set forth in the General Schedule for Electronic Records published by the Department of Cultural Resources or as required by Federal (e.g. IRS 1075, HIPAA, FERPA, etc.), State or Departmental requirements; whichever is longest;
- Retained and archived in a manner that will protect the integrity of the data stored on the chosen media for as long as requirements mandate; and
- Appropriately destroyed upon the expiration of retention requirements (see 5.5.3 Sanitize Media).

3.6.1 HIPAA Retention Requirements

45 CFR 164.316(b)(1) requires DHHS Divisions and Offices to "maintain the policies and procedures implemented to comply with this subpart in written (which may be electronic) form; and (ii) if an action, activity or assessment is required by this subpart to be documented, maintain a written (which may be electronic) record of the action, activity, or assessment."

Additionally, 45 CFR 164.316(b)(2)(i) requires DHHS Divisions and Offices to "retain the documentation required by paragraph (b)(1) of this section for 6 years from the date of its creation or the date when it last was in effect, whichever is later."

Guidelines

Divisions and Offices are responsible for managing their records in accordance with identified requirements regardless of where they reside. Because of this when dealing with external third-parties that will manage or maintain records on behalf of, or as part of a

Department system; contracts and agreements should include language identifying roles and responsibilities related to records management.

3.7 Isolating Health Care Clearinghouse Functions

If during the HIPAA determination process an organization within DHHS is determined to be a health care clearinghouse, the then identified clearinghouse must implement policies, procedures and technical safeguards that isolate and protect the electronic protected health information of the clearinghouse from unauthorized access by other entities within DHHS.

-- Remainder of Page Intentionally Left Blank –

CHAPTER 4: SYSTEM ACQUISITION, DEVELOPMENT AND MAINTENANCE

All systems, including software as a service (SaaS), whether acquired or developed must be implemented and maintained with the safeguarding of data in mind. Security requirements should be identified, agreed upon and documented as part of the overall business case throughout the system's lifecycle, and not bolted on afterward.

4.1 System Development Life Cycle (SDLC)

To ensure reliable and stable systems that provide adequate security controls, all Divisions and Offices developing software applications are required to have a documented and repeatable SDLC methodology, including process, which support/complement their business needs.

SDLC methodologies that can be used by Divisions and Offices as a foundation to effectively develop a system include but are not limited to waterfall, prototyping, spiral, and rapid application development (RAD). The expected size and complexity of the system, development schedule, and length of a system's life should be considered when deciding a SDLC methodology.

Guidelines

Divisions and Offices' SDLC shall, at a minimum, include the following five phases*:

- **Phase I - Initiation:** the need for a system is expressed and the purpose of the system is documented
- **Phase II - Development/Acquisition:** the system is designed, purchased, programmed, developed, or otherwise constructed
- **Phase III - Implementation/Assessment:** after system acceptance testing, the system is installed or fielded
- **Phase IV - Operation/Maintenance:** the system is performing in an operational state; the system is almost always modified by the addition of hardware and software and by numerous other events
- **Phase V - Disposal:** activities conducted during this phase ensure the orderly termination of the system, safeguarding vital system information, and migrating data processed by the system to a new system, or preserving it in accordance with applicable records management regulations and policies

* Phases may continue to be repeated throughout a system's life prior to disposal based on the chosen SDLC methodology.

To ensure privacy and data protection is incorporated into the SDLC process, Divisions and Office's SDLC shall, at a minimum, include the following data protection steps into the five phases mentioned above:

- **Phase I - Requirements:** Perform an initial Privacy Threshold Assessment (PTA) and Privacy Impact Analysis (PIA); Review privacy and information security policies, standards, and controls to ensure they are following requirements for collection, use, retention, and disposal of personal data
- **Phase II - Design:** Minimize data and perform a formal PTA and PIA; analyze relevant privacy controls to ensure they are designed, developed, and implemented; design and implement feedback control privacy mechanisms into system
- **Phase III - Develop:** Obtain initial data subject consent on personal data collection, use, disclosure and retention; ensure transparency where data subjects understand systems and process; ensure data subjects are informed on how to access their personal data and ensure it is up to date and accurate; implement security measures to ensure protection of personal data; perform ongoing testing and evaluation
- **Phase IV - Test:** Monitor and report privacy controls through periodic testing and evaluation
- **Phase V - Deploy:** Integrate new privacy protection methods or controls into systems for improved privacy; analyze privacy policies, standards and procedures and system performances for irregularities
- **Phase VI- Maintenance:** Ensure proper management of new applications and technology in production.

4.2 Secure Coding Standards

Developer(s), to the extent possible, must ensure programming language(s) and the associated code used for system development does not include known vulnerabilities (e.g. stack or buffer overflows, Structured Query Language (SQL) injection, etc.) that could lead to system compromise or failure.

Divisions and Offices should develop a uniform set of standards and guidelines by which source code can be evaluated for conformance with performance, reliability and security requirements, providing developers/programmers a foundation to create secure systems.

Guidelines

Secure coding standards should seek to improve software and source code by:

- Reducing the number of software bugs and problems
- Enforcing comprehensible (i.e., readable and understandable) code
- Reducing redundancy by using existing code that is tested and proven to be secure
- Ensuring code provides a predictable response (i.e., execution of code in a defined state despite unexpected inputs or actions)
- Requiring input validation
- Where possible preventing confidential data from being stored on client systems
- Creating error messages that do not return system specific information that could be leveraged for malicious purposes to the users
- Promoting the use object, inheritance, encapsulation, and polymorphism wherever possible
- Encouraging prudent use of environment variables

4.2.1 Securing System Development Code

Program libraries, source repositories, applications and code used for developmental purposes shall be stored and run on separate hosts either physical or virtual from production systems.

Access to, including the ability to copy, view or download, developmental resources requires explicit authorization from the system owner. Development resources shall have detailed content and activity reports, audit trails and formal procedures (e.g. archiving and removal code that has been superseded or discontinued).

4.3 Security for Systems Contracts

Specific security requirements (e.g. regulatory requirements such as HIPAA, FERPA, and SSA) shall be identified and documented in all system Requests for Information (RFI), Quote (RFQ) and Proposal (RFP) and in final contracts.

Guidelines

Divisions and Offices should at a minimum include a qualifying security language within all applicable contractual/procurement documents. An example of this language would be:

> **Protection of Confidential Information**
>
> Any confidential information provided to the contractor by the department or developed by the contractor based on information provided by the department in the performance of this agreement shall be kept confidential and shall not be made available to any individual or organization by the contractor without the prior written approval of the persons listed in (point to whatever list of points of contact you have within the RFP). Upon termination of this agreement, contractor shall deliver all confidential information in its possession to the department.
>
> The contractor agrees to protect the confidentiality of all confidential information and not to publish or disclose such information to any third party without the department's written permission.
>
> The contractor must not disclose confidential Information of the department or of the State of North Carolina to a subcontractor unless and until such subcontractor has agreed in writing to protect the confidentiality of such confidential information in the manner required of the contractor under this agreement.
>
> The contractor shall comply with applicable federal, state, and department regulations, policies standards and procedures.

Accountability for Breaches

Upon the suspicion or the discovery of a breach of security of confidential information, the contractor shall notify the persons listed in (point to whatever list of points of contact you have within the RFP). The contractor shall comply with applicable federal, state, and department incident response procedures.

-- Remainder of Page Intentionally Left Blank –

CHAPTER 5: LIFE CYCLE SECURITY MANAGEMENT

Life cycle security management helps define security throughout all phases of both the Project Life Cycle (PLC) and System Development Life Cycle (SDLC), ensuring that security was considered in all phases.

At the department level life cycle security management is incorporated into a linear sequential model allowing for a parallel between SDLCs and the State's PLC to be drawn. Due to the simplicity of this model the concepts defined here can be translated and adapted to any life cycle model.

Documentation associated with life cycle security, as well as the model itself, can be used for oversight (i.e., why decisions were made) or by third-party reviewers as verification of system security controls (e.g. system is actually being safeguarded, operated and maintained as required).

Executing a risk management-based approach for systems and projects means integrating security early and throughout the software and project life cycles. Integration enables security to be planned, acquired, built in, and deployed as an integral part of a project or system. It plays a significant role in measuring and enforcing security requirements throughout the phases of the life cycle.

Major security tasks in each phase are identified and defined in the following areas:

- Activities: The description provides a detailed overview of the activity and highlights specific considerations necessary to address the task
- Outputs: Common task deliverables and artifacts are listed along with suggestions for forward/backward integration of these work products
- Synchronization: A feedback loop that provides opportunities to ensure that the SDLC/PLC is implemented as a flexible approach that allows for appropriate and consistent communication and the adaptation of tasks and deliverables as the system is developed
- Interdependencies: This section identifies key interdependencies with other tasks to ensure that security integration activities are not negatively impacted by other processes
- Guidance: Non-mandatory suggestions and enhancements to assist in the implementation of activities and outputs

5.1 SDLC: Initiation / PLC: Initiation

During this first phase of the development life cycle, security considerations are key to diligent and early integration, thereby ensuring that threats, requirements, and potential constraints in functionality and integration are considered. At this point, security is looked at more in terms of business risks with input from security representative (e.g. a political risk identified as a result of a prominent website being modified or made unavailable during a critical business period, which may result in decreased trust by citizens).

Key security activities for this phase include:

- Initial delineation of business requirements in terms of confidentiality, integrity, and availability
- Determination of information categorization and identification of known special handling requirements to transmit, store, or create information such as personally identifiable information
- Classification of data used, stored, maintained and processed by the system

Early planning and awareness will result in cost and time saving while assisting in proper risk management planning. Security discussions should be performed as part of (not separately from) the development project to ensure solid understandings among project personnel of business decisions and their risk implications to the overall development project.

This early involvement will enable the developers to plan security requirements and associated constraints into the project. It also reminds project managers that many decisions being made have security implications that should be weighed appropriately, as the project continues.

5.1.1 Initiate Security Planning

Activities:

Identification of Security Roles
Divisions and Offices must identify both a Data Steward and Custodian (see 3.3 Roles and Responsibilities Related to Data Management) for the system, taking into consideration the amount of time and skills needed to effectively carry out the responsibilities of each role. Early identification of security roles allows assigned individual(s) to provide valuable insight into risk-based decisions made early in the process and provides supporting protocols for security integration into the system's development cycle.

Stakeholder Security Integration Awareness
The Data Steward and Custodian will ensure all key stakeholders (e.g. business owner, developers, programmers, etc.) have a common understanding, including security implications, considerations, and requirements such as: roles and responsibilities related to security, and the identification of security requirements (i.e., relevant laws, regulations, and standards).

Initial Project Planning
Security milestones, timeframes and triggers must be integrated into the project outline and schedule during initial development to allow for proper planning as changes occur. During this phase, activities may be more in terms of decisions followed by security activities.

Outputs:

- Data Steward and Custodian identification
- Supporting documents (slides, meeting minutes, etc.)
- Common understanding of security expectations
- Initial schedule of security activities or decisions

Synchronization:

A series of security meetings should be planned to discuss each of the security considerations throughout the system development.

Interdependencies:

A project schedule should integrate security activities to ensure proper planning of any future decisions associated with schedules and resources.

Guidance:

- Many of the project initiation outputs (i.e., meeting minutes, briefings, role identification, etc.) can be standardized and used to assist in level-of-effort planning
- In-person meetings can provide opportunities to gauge security understanding and awareness
- In the event the same individual is identified as a Data Steward or Custodian for multiple systems, a planned approach will increase their ability to multi-process (e.g. assigning common systems)

5.1.2 Categorize the Information System

Activities:	Security categorization establishes the foundation for security among systems. **Identify Information Types** Divisions and Offices shall identify all of the applicable information types that are representative of data input, stored, processed or output from a system through the creation of a data flow diagram (see 3.4 Data Flow Diagram Development). **Establish Security Categorization** Security categories are assigned by selecting and adjusting appropriate values (i.e., High, Moderate, Low and Not Applicable) for the potential impact (i.e., jeopardize the information needed by the system to accomplish its mission, fulfill legal responsibilities, maintain day-to-day functions and protect individuals) of compromises to the confidentiality, integrity, and availability to system data.
Outputs:	• Initial development of Data Flow Diagram • Security Categorization - Essential to the security categorization process is documenting the research, key decisions, and supporting rationale for the information system security categorization (included in the System Security Plan). • High-Level Security Requirements • Level-of-Effort Estimates - Initial level of effort can be derived from minimal security controls identified through the risk assessment process as defined in 6.5 Level of Effort Estimation
Synchronization:	The security categorization should be revisited if there are significant changes to the information system or when the business impact analysis is updated.
Interdependencies:	• Business Impact Analysis (BIA): Because security categorization and BIA share common objectives the cross-utilization of each should be considered to support accuracy • System Design: Understanding data types and security categorization level allows for systems to be designed with economies of scale and protection • Continuity of Operations Planning (COOP): COOP personnel should review system documentation to ensure correct contingency and disaster protection security controls and avoid the over protection of lower-impact systems • Information Sharing and System Interconnection Agreements: Security categorization should be utilized when assessing intersystem connections or data sharing
Guidance:	6.2.1 System Security Risk Assessment will assist Divisions and Offices in making the appropriate selection of security controls for their systems and establish the security categorization of the system.

5.1.3 Assess Business Impact

Activities:	An initial Business Impact Assessment (BIA) must be conducted detailing how the system and its components correlate to identified critical business services supported by the system, and the impact (i.e., consequences) on those services due to a disruption.

Outputs:	• Identify lines of business supported by the system and how those lines of business will be impacted • Identify core system components needed to maintain minimal functionality • Initial identification of the system's Recovery Time Objective (RTO - the length of time the system can be down before the business is impacted) • Initial identification of the Recovery Point Objective (RPO - the business tolerance for loss of data)
Synchronization:	The BIA should be reviewed and updated throughout the systems life cycle as development decisions (e.g. new functionalities) are added or when the system's purpose/scope change significantly.
Interdependencies:	• The BIA process is a key step in the system contingency planning, including requirements and mitigating solutions, and allows for improved identification of system requirements, processes and interdependencies • System Security Categorization activities are similar in terms of purpose. Information provided during those activities can be used to assist in BIA efforts
Guidance:	• Initially, information from the original business case can be used to populate the BIA • The BIA should also take into account the availability impact level identified during the security categorization activity • Larger, more complex developments, should consider holding a stakeholders' meeting to brainstorm possible linkages and impacts • Reuse data and information for multiple purposes when applicable. Categorization decisions can be reused for BIA, disaster recovery (DR), contingency planning (CP), and continuity of operations (COOP) decisions. Categorization should be reflective of DR priorities. If not, there is potential that categorization was not conducted at an appropriate level or DR priorities are incorrect • BIA results can be used to assist in developing requirements or objectives for service-level agreements (SLAs)

5.1.4 Data Classification Assessment

Activities:	When developing a new system, it is important to directly consider if the system will transmit, store, or create information that may be considered confidential. This determination is typically done in parallel with the security categorization process when identifying information types.
Outputs:	Classification of data collected, stored, or created within the system as confidential or public and the documented regulation(s) defining the classification.
Synchronization:	Data classification should be reviewed and updated as major decisions affecting what data is collected, stored, or created within the system change.
Interdependencies:	• Data classification is reflected in the security categorization process as part of identification of baseline security controls • The System Security Plan, Contingency Plan, and Business Impact Assessment should capture system data classification levels
Guidance:	Chapter 3.2.1 Data Classification assists Divisions and Offices in classifying system data appropriately.

5.2 SDLC: Development/Acquisition / PLC: Planning and Design

This section addresses security considerations unique to the second SDLC/PLC phase.

Key security activities for this phase include:

- Conduct the risk assessment and use the results to supplement the baseline security controls
- Analyze security requirements
- Perform functional and security testing
- Prepare initial documents for system certification and accreditation
- Design security architecture

Although this section presents the information security components in a sequential top-down manner, the order of completion is not necessarily fixed. Security analyses of complex systems will need to be iterated until consistency and completeness is achieved.

5.2.1 Assess System Risk

Activities:	The purpose of a risk assessment is to evaluate current knowledge of the system's design, stated requirements, and minimal security requirements derived from the security categorization process to determine their effectiveness to mitigate anticipated risks. Results should show that specified security controls provide appropriate protections or highlight areas where further planning is needed. To be successful, participation is needed from people who are knowledgeable in the disciplines within the system domain (e.g. users, technology experts, operations experts).
Outputs:	A refined risk assessment based on a mature system design that accurately reflects potential risks to the system, and assists in the identification of design weaknesses, project constraints to both business and system components.
Synchronization:	Once the risk assessment is completed it may be necessary to revisit previously-completed Security Planning efforts.
Interdependencies:	Security categorization provides the baseline security level that is used for identification of required security controls as part of the risk assessment.
Guidance:	• Chapter 6: Risk Management provides guidance to Divisions and Offices on conducting risk assessments • Risk assessments should be conducted prior to the approval of design specifications as it may result in additional specifications or provide further justification for specifications • Consideration should be given to how the system might affect or be affected by other systems to which it will be directly or indirectly connected including identifying and addressing shared and inherited risks • The system should leverage common security controls where available to assist in risk mitigation • During the risk assessment process previous requirements should be transitioning into system specific controls • As new functional requirements are identified, specific security analyses should be conducted to prevent the introduction of additional risk or weakening of existing security controls • The results of the risk assessment can be used to develop requirements or objectives for service-level agreements (SLAs) with supporting service providers

5.2.2 Select and Document Security Controls

Activities:	**Security Control Identification** The selection of security controls consists of three activities: • The selection of baseline security controls (including common security controls) • The application of security control tailoring guidance to adjust the initial security control baseline • The supplementation of the tailored baseline with additional controls based on an assessment of risk and local conditions **Security Control Documentation** Identified security controls are to be documented within the system's Security Plan and signed off by appropriate authorizing individuals within the organization.
Outputs:	System Security Plan – Serves as an overview of the security requirements for the system and its components by describing the security controls in place, or planned, for meeting those requirements, the rationale for security categorization, how individual controls are implemented within specific environments, and situational system usage restrictions.
Synchronization:	Security controls and associated specifications should appropriately reflect the level of safeguards required in line with the system categorization and data classification. When making decisions related to security controls, consideration must be given to secondary risks that may result from how current decisions influence previously decided security controls identified during the risk assessment.
Interdependencies:	• Once formulated, security control requirements must be incorporated into the System Security Plan. • The risk assessment is the primary means by which Divisions and Offices shall identify security controls for systems.

Guidance:	• Addressing security requirements in a matrix format can assist in reviews, control implementation and aid in gap/risk analysis • Security requirements should be stated in specific terms. For complex systems, iterations of the requirements analysis may be needed. If so, planned reviews should occur at major identified milestones • More detailed "attack prevention" requirements will also help to ensure that security controls and methods are tested prior to release, if required • Security controls are not one-dimensional and should be addressed as appropriately on multiple components throughout the system • Disposition planning should begin during this phase and be planned for throughout all remaining phases of the life cycle • The number and type of appropriate security controls and their corresponding system components may vary throughout a particular system's development and procurement life cycles • How security controls are blended is directly tied to the role of the system and its support of the organization's mission

5.2.3 Design Security Architecture

Activities:	At the enterprise level, the system should be reviewed to ensure that it does not conflict or unnecessarily provide redundant services. At the system level, security should be architected and then engineered into the design of the system. This may be accomplished by zoning or clustering services either together or distributed for either redundancy or additional layers of protection. Security designing at the system level should take into consideration services obtained externally, planned system interconnections, and the different orientations of system users (e.g. customer service versus system administrators). Minimal security requirements as well as requirements and constraints determined early in the process should provide architects with a set of assumptions and constraints to build around.
Outputs:	• Schematic of security integration providing details on where, within the system, security is implemented and shared. Security architectures should be graphically depicted and detailed in the Security Plan to the extent the reader can see where the core security controls are applied and how • Listing of shared services and resulting shared risk • Identification of common controls used by the system
Synchronization:	• The security architecture is a key component of the system documentation (e.g. Security Plan) that should be reviewed and maintained as major changes or significant control gates (milestones) are reached • Significant results from assessments, security testing, and reviews should be examined for potential feedback on effectiveness

Interdependencies:	• Architecture should provide insights into other like systems, controls or services where integration could optimally occur • The systems Security Plan will document the summary of the security architecture approach or strategy • Security requirements analysis will provide the majority of the information at the detailed level required to determine if the security architecture will work as intended or if gaps or unnecessary redundancy exist
Guidance:	• Security architecting can assist in determining effective compensating or use of common controls when there are issues with implementing minimal security requirements with the system's design specification • Demonstrating the logic behind the security of this system will help in determining the need for additional controls • Risks accepted by the system that may have downstream, adverse effects on the enterprise can be identified and raised as issues during the architectural review. Enterprise risk culminating from all individual system risk should be expressed and tracked through the architecture process • In addition, as the system matures and more decisions are made as to services utilized, the system should be reviewed for optimal integration where applicable

5.2.4 Engineer in Security and Develop Controls

Activities:	During this stage, security controls are implemented and become part of the system with the intent to identify challenges to system performance early. During this task, decisions are made based on integration challenges and trade-offs. It is important to document the major decisions and their business/technology drivers. In cases where the application of a planned control is not possible or advisable, compensating controls should be considered and documented.
Outputs:	• Implemented controls with documented specification for inclusion into the Security Plan • List of security control variations resulting from development decisions and tradeoffs • Potential assessment scenarios to test known vulnerabilities or limitations
Synchronization:	Security control application may undergo changes as a result of functional and user testing. Changes should be documented and the Security Plan updated appropriately.
Interdependencies:	• Security requirements analysis should be reviewed and updated if change is needed • Security architecture strategy should be reviewed and updated if change is needed • Specific configurations should be documented or referenced in the System Security Plan
Guidance:	• Documenting security deviations from initial security requirements at this stage demonstrates and encourages solid risk planning; reduce time later by eliminating the backtracking of business justifications. • The application of security controls during development should be carefully considered and logically planned as some security controls may limit or hinder development activities

-- Remainder of Page Intentionally Left Blank –

5.2.5 Develop Security Documentation

Activities:	At this stage, it is important to solidify the security approach, scope, and understanding of responsibilities through defined documentation including but not limited to: • System Security Plan • Configuration Management Plan • Business Continuity Plan (BCP) including a BIA • Continuity of Operations Plan (COOP) • Continuous Monitoring Plan • Security Education, Training, and Awareness, (SETA) Plan • Incident Response Plan
Outputs:	Additional security documentation supporting the System Security Plan.
Synchronization:	These documents will need to be updated toward the end of user acceptance testing to ensure that they are accurate.
Interdependencies:	System security documentation should align with: • Security requirements analysis • Security architecture • Business impact assessment • Security categorization
Guidance:	• Security operations should not be driven by documentation of compliance but rather based on system need and compliance through security guidance • Systems that are large in size, complex in design, or by nature sensitive, it is best to assign a single point of contact (POC) to each document to initiate a meeting on the document's scope, expectations, and level of granularity • During the development of security documents one should consider the maturity of the security being documented. In some cases, documents may contain only known requirements, common controls or templates

-- Remainder of Page Intentionally Left Blank –

5.2.6 Conduct Testing (Developmental, Functional and Security)

Activities:	Systems being developed or undergoing software, hardware, and/or communication modification(s) must be tested and evaluated prior to being implemented. The objective of the test and evaluation process is to validate that the developed system complies with the functional and security requirements. Testing of security controls is based on technical security specifications for those controls identified in section 6.2.1 System Security Risk Assessment. The testing processes should focus on: • Specificity, the testing must be scoped to test the relevant security requirement as it is intended for use in its environment • Repeatability, the testing process must be capable of the execution of a series of tests against an information system more than once (or against similar systems in parallel) and yield similar results each time • Iteration, each system will be required to execute functional tests in whole or in part a number of successive times in order to achieve an acceptable level of compliance with the requirements of the system
Outputs:	Documentation of test results, including any unexpected variations discovered during testing.
Synchronization:	All test results are returned to developers for configuration-managed updates. Unexpected results may require additional clarification based on the nature of the tested requirement.
Interdependencies:	• Security requirements analysis may be impacted and require updating • Changes may impact the security architecture and require updating • The system risk assessment may need updating to accurately reflect changes in mitigations or requirements

Guidance:	• Only test (i.e., fake) or de-identified data should be used during system development Absolutely no operational, security-relevant, or PII should reside within any system or software during development • In an effort to reduce redundant functional and security testing activities, it is recommended that functional test plans include general security features testing (to the greatest extent possible) • Preliminary testing of basic security controls during functional testing may reduce or eliminate issues earlier in the development cycle (e.g. mandatory access controls, secure code development, and firewalls) • For systems of high visibility and sensitivity, independent development testing may be recommended • To the degree possible functional testing should be automated to ensure that the test process is repeatable and iterative • Capture the process and results of all security testing that occurs throughout the life cycle for evaluation, issue identification, potential reuse, and cost/risk mitigation • Source code should be periodically reviewed using automated tools or manual spot check for common programming errors that have a detrimental impact on system security including but not limited to: cross-site scripting vulnerabilities, buffer overflows, race conditions, object model violations, poor user input validation, poor error handling, exposed security parameters, passwords in the clear, and violations of stated security policy, models, or architecture

5.3 SDLC: Implementation/Assessment / PLC: Execution and Build

During the SDLC: Implementation/Assessment and the PLC: Execution and Build phase, the system will be installed and evaluated in the organization's operational environment.

Key security activities for this phase include:

- Integrate the information system into its environment
- Plan and conduct system certification activities in synchronization with testing of security controls
- Complete system accreditation activities

5.3.1 Integrate Security into Established Environments or Systems

Activities:	Integration occurs at the operational site when the system is being prepared for deployment in production. Security control settings are enabled in accordance with manufacturer's instructions, available security implementation guidance, and documented security specification.
Outputs:	• Verified list of operational security controls • Completed System Documentation

Synchronization:	• Issues encountered during installation should be evaluated for inclusion into the contingency plans based on the potential for reoccurrence • System security controls should be reviewed for compliance and proper configuration, and a verified list provided to the system owner.
Interdependencies:	Appropriate security documentation (e.g. Security Plan, BCP, and Configuration Management) should be updated to reflect system operational configurations.
Guidance:	• Test and development environments should be cleared of data that is no longer required • Integration and acceptance testing should occur after system delivery and installation • Care should be exercised when integrating systems into operational environments to ensure that critical operations are not disrupted

-- Remainder of Page Intentionally Left Blank –

5.3.2 Assess System Security

Activities:	Systems being developed or undergoing software, hardware or communication modification(s) must be assessed prior to being granted accreditation and placed in an operational (i.e., production) state. The objective of the security assessment process is to validate that the system security controls are implemented, operating as intended, producing the desired outcome and will operate within an acceptable level of residual security risk. In addition, periodic testing and evaluation of the security controls in an information system must be conducted to ensure continued effectiveness.
Outputs:	• Security Authorization Package, which includes the security assessment report, a plan of action and milestones, and the updated System Security Plan
Synchronization:	• Certifier provides written documentation of System Certification to system owner, Data Steward and Data Custodian • Assessment results are shared with system owner, Data Steward, Data Custodian, system administrator, and developers as required
Interdependencies:	All previous steps.
Guidance:	• All documentation should be in final review stages to ensure a current snapshot of the system • Assigning a core team of representatives from the major stakeholders to meet throughout testing will assist in communication and reduce surprises • Chapter 9: System Authorization articulates the authorization process • Section 6.3.1 provides guidance on the creation of a plan of action and milestones • Prioritize continuous monitoring by risk and cost-effectiveness • Reuse prior and relevant assessment results as possible • Testing of security controls should be based on defined procedures as in section 7.5 Security Assessments and Monitoring.

-- Remainder of Page Intentionally Left Blank –

5.3.3 Authorize the Information System

Activities:	System authorization (i.e., accreditation) is granted by the identified organization executive sponsor, and is based on the verified effectiveness of security controls to some agreed-upon level of assurance and an identified residual risk to departmental assets or operations (including mission, function, image, or reputation).
Outputs:	A documented Security Authorization Decision from Authorizing Official to system stakeholders (e.g. system owner, Data Steward and Custodian).
Synchronization:	System inventories and reporting statistics should be updated to reflect the accredited status.
Interdependencies:	• Update security and budget documentation with resulting status • System certification statement
Guidance:	• Authorizing individuals need to make risk decisions not only for the system, but for the risk extended to the organization as a whole by placing the system into operation • The security authorization decision is a risk-based decision that depends heavily, but not exclusively, on the security testing and evaluation results produced during the security control verification process • Authorizing individuals should leverage the completed System Security Plan and security test and evaluation results

5.4 SDLC: Operations and Maintenance / PLC: Implementation

SDLC: Operations and Maintenance and PLC: Implementation is the fourth phase. In this phase, systems are in place and operating, enhancements or modifications to the system are developed and tested, and hardware or software is added or replaced. The system is monitored for continued performance in accordance with security requirements and needed system modifications are incorporated. The operational system is periodically assessed to determine how the system can be made more effective, secure, and efficient. Operations continue as long as the system can be effectively adapted to respond to an organization's needs while maintaining an agreed-upon risk level. When necessary modifications or changes are identified, the system may reenter a previous phase of the SDLC/PLC.

Key security activities for this phase include:

- Conduct an operational readiness review
- Manage the configuration of the system
- Institute processes and procedures for assured operations and continuous monitoring of the information system's security controls
- Perform reauthorization as required

5.4.1 Review Operational Readiness

Activities:	Many times when a system transitions to a production environment, unplanned modifications to the system occur. If changes are significant, a modified test of security controls, such as configurations, may be needed to ensure the integrity of the security controls. This step is not always needed; however, it should be considered to help mitigate risk and efficiently address last-minute surprises.
Outputs:	Evaluation of security implications due to any system changes.
Synchronization:	• System Administrators along with the Data Steward and Custodian confirm to System Owner that system is operating normally and compliant with security requirements • Should a last-minute change occur that fundamentally changes the level of risk to the system, the system owner should consider recertification - this is rare.
Interdependencies:	• An operational readiness review supplements the certification and authorization process to ensure that changes are reviewed for risk potential • Any change to security controls should be updated in the security documentation (e.g. System Security Plan)
Guidance:	• When an application is enhanced or changed, regression testing helps to ensure that additional vulnerabilities have not been introduced (e.g. adding source code can introduce errors in some areas or negatively impact existing and stable functions) • Changes that include additional data fields should be noted and analyzed to determine if the security posture of the system has degraded or introduced a need for additional controls • Ensure users are adequately trained on security awareness and practices for the system functions prior to operational deployment

-- Remainder of Page Intentionally Left Blank –

5.4.2 Configuration Management and Control

Activities:	Changes to the hardware, software, or firmware of a system can have a significant security impact. Configuration management and control procedures are critical to establishing an initial baseline of hardware, software, and firmware components for the system and subsequently for controlling and maintaining an accurate inventory of any changes to the system. Documenting system changes and assessing the potential impact on the security of the system on an ongoing basis is an essential aspect of maintaining the security accreditation, and when implemented effectively, provides vital input into the system's continuous monitoring capability (e.g. aids in the identification of significant changes that alter a system's security posture and control effectiveness to ensure proper assessment and testing occurs).
Outputs:	• System configuration management and control procedures • Updated security documentation (e.g. System Security Plan, BCP) • Security evaluations of documented system changes
Synchronization:	• System updates should be included into the system's security documentation (e.g. System Security Plan, BCP) at least annually or with significant change • System configuration management documents should provide input into the Continuous Monitoring plan for the system
Interdependencies:	The System Security Plan, including the security architecture, should provide key details on component-level security services, which in turn can assist in providing a benchmark to evaluate the impact of the planned change as it relates to security requirements.
Guidance:	• Individuals responsible for reviewing system changes should keep in mind how/if any changes would directly or indirectly impact the confidentiality, integrity, and availability of data • Some system enhancements that add new data may require a review of impact to the system security categorization and associated security controls • Abbreviated change management processes allowing for unique emergency situations should be identified for emergency purposes; however these situations should always be followed up with a full review when time permits • Configuration Management procedures should be designed to ensure repeatability and consistency

5.4.3 Continuous Monitoring

Activities:	The objective of continuous monitoring is to determine if the security controls in place continue to be effective over time in light of system changes that occur, as well as the environment in which the system operates. The ongoing monitoring of security control effectiveness can be accomplished in a variety of ways, including security reviews, self-assessments, configuration management, antivirus management, patch management, security testing and evaluation, or audits. Automation should be leveraged where possible to reduce level of effort and ensure repeatability. The Department shall ensure its compliance with the Statewide Information Security Manual. The State Chief Information Officer (SCIO), shall ensure State agencies and State data are operating in compliance with established enterprise security standards. The Continuous Monitoring Plan shall monitor and ensure that all agencies are assessed using one or a combination of assessment methods: • Third Party Independent Assessment (Vendor or National Guard) are performed every three (3) years • Self-Assessments are performed annually The annual assessments and compliance reporting will allow the monitoring of cyberdeficiencies. Firewalls are managed at the DIT level, applications are backlists/ whitelisted at DIT. Any software applications identified as unauthorized or "blacklisted" will be provided by the NCDIT as necessary. The "blacklisted" software applications will be removed from applicable Divisions and Offices. Included as a part of continuous monitoring is reauthorization which occurs when there are significant changes to the system affecting the security of the system or every three (3) years.
Outputs:	• Documented results of continuous monitoring • Security reviews, metrics, measures, and trend analysis • Updated security documentation and security re-accreditation decision, as necessary
Synchronization:	Continuous monitoring should be adjusted as risk levels fluctuate significantly and security controls are modified, added, and discontinued.
Interdependencies:	Continuous monitoring provides system owners with an effective tool for producing ongoing updates to information System Security Plans, security assessment reports, and plans of action and milestones documents.

Guidance:	• The State Continuous Monitoring Plan requires all cloud vendors annually report and document their compliance posture. These vendors include those providing Infrastructure as a Service (IaaS), Platform as a Service (PaaS) or Software as a Service (SaaS). • Vendor annual reporting documents shall be specified in the vendor contract language. • Where applicable/available, a continuous monitoring program should make use of common services for more frequent monitoring, as well as system-specific monitoring for critical security controls • Realizing that it is neither feasible nor cost-effective to monitor all of the security controls in any system on a continuous basis, Divisions and Offices should consider establishing a schedule for security control monitoring to ensure that all controls requiring more frequent monitoring are adequately covered and that all controls are covered at least once between each accreditation decision • Continuous monitoring processes should be evaluated periodically to review changes in threats and how this could affect the ability of controls to protect a system. These threat updates may result in updated risk decisions and changes to existing controls • Take credit for activities already underway that count for continuous monitoring (anti-virus data file updates, routine maintenance, physical security fire drills, log reviews, etc., should all be identified and captured in the continuous monitoring phase) • Prioritize continuous monitoring by importance of control to mitigating risk, validation of milestone items that become closed and single control points of failure • Look at a monitoring cycle that will coincide with the system certification life span and capture test procedures and results for reuse upon recertification • Continuous monitoring activities can provide useful data to support security performance plans and measures of security return on investment (ROI) • A well-designed and well-managed continuous monitoring process can provide essential, near real-time security status information that can be used to take appropriate risk mitigation actions and make credible, risk-based authorization decisions regarding the continued operation of the system and the explicit acceptance of risk that results from that decision

5.5 SDLC: Disposal / PLC: Closeout

The final phase in the SDLC/PLC is Disposal and Closeout, providing for the disposal of a system and closeout of any contracts in place. Security issues associated with data and system disposal should be explicitly addressed. When systems are transferred, become obsolete, or are no longer usable, it is important to ensure that departmental resources and assets are protected.

Usually, there is no definitive end to a system. Systems normally evolve or transition to the next generation because of changing requirements or improvements in technology. System Security Plans should continually evolve with the system. Much of the environmental, management, and operational information should still be relevant and useful in developing the Security Plan for the follow-on system.

The disposal activities ensure the orderly termination of the system and preserve the vital information about the system so that some or all of the data may be reactivated in the future, if necessary. Particular emphasis is given to proper preservation of the data processed by the system so that the data is effectively migrated to another system or archived in accordance with applicable records management regulations and policies for potential future access.

Key security activities for this phase include:

- Build and Execute a Disposal/Transition Plan
- Archive of critical information

- Sanitization of media
- Disposal of hardware and software

5.5.1 Build and Execute a Disposal/Transition Plan

Activities:	Building a disposal/transition plan ensures that all stakeholders are aware of the future plan for the system and its data. This plan should account for the disposal/transition status for all critical components, services, and data. Much like a work plan, the disposal/transition plan identifies necessary steps, decisions, and milestones needed to properly close down, transition or migrate the system or its data.
Outputs:	Documented disposal/transition plan for closing or transitioning the system and its data.
Synchronization:	Security documentation should reflect pending plans if security decisions and funding are reallocated or otherwise impacted because of the disposal decision.
Interdependencies:	Security documentation such as the Security Plan and security control requirements may need updating.
Guidance:	• Sometimes disposed systems have remained dormant but still connected to infrastructure. As a result, these components are often overlooked, unaccounted for, or maintained with suboptimal security controls creating additional and unnecessary risk to the infrastructure and all connected systems • Prior to data disposal, System Owners must ensure compliance with applicable record retention regulations • Do not wait for the disposal phase to make a disposal/transition plan. Plan for disposal/transition throughout all phases of the life cycle, as hardware and software become obsolete or damaged

5.5.2 Ensure Data Preservation

Activities:	Divisions and Offices must document system data preservation methods taking into consideration future requirements for retrieving information (e.g. technology and encryption mythologies), along with the retention requirements.
Outputs:	Index of preserved information, and its location and retention attributes.
Synchronization:	Records management and retention requirements must be considered.
Interdependencies:	Security and privacy considerations for the data or activities as it relates to the Freedom of Information Act.
Guidance:	• Data shall be managed in accordance with Chapter 3.6 Records Management • Divisions and Offices should consult with the North Carolina Department of Cultural Resources, Government Records Branch, to select archival media that will protect the integrity of the data stored on those media for as long as the data are archived • Divisions and Offices should conduct s risk analysis (see Chapter 6.2 Assessing Risk) to determine if the encryption of data at rest is required or feasible. • NIST publication 800-111 titled “Guide to Storage Encryption Technologies for End User Devices” provides additional information on the encryption of data at rest.

-- Remainder of Page Intentionally Left Blank –

5.5.3 Sanitize Media

Activities:	Divisions and Offices must track, document, and verify media sanitization and destruction actions while periodically testing sanitization equipment/procedures to ensure correct performance, and prevent unauthorized individuals from gaining access to and using the information contained on the media after disposal or reuse. **Public (i.e., non-confidential) Data** Non-confidential data can be sanitized through Disposal (i.e., the act of discarding media with no other sanitization considerations). This is most often done by paper recycling containing nonconfidential information but may also include other media. **Confidential Hard Copy Data** Hard copy records and data shall be sanitized following the requirements set forth by the Department of Cultural Resources in NC Administrative Code, Title 7, Chapter 4, Subchapter M, Section .0510 (May 16, 1989). **Confidential Electronic Data** System digital media shall be sanitized through Clearing (e.g. overwriting storage space on the media with non-sensitive data), Purging (e.g. degaussing, secure erasing) or Destruction (e.g. disintegration, incineration, pulverization and shredding).
Outputs:	Media sanitization records
Synchronization:	None
Interdependencies:	Security categorization provides the identification and associated risk level of system information.
Guidance:	• The cost versus benefit of a media sanitization process should be understood prior to a final decision (e.g. it may not be cost-effective to degauss inexpensive media) • The selected process should be assessed as to cost, environmental impact, etc., and a decision made that best mitigates the risk to confidentiality and that best satisfies other constraints imposed on the process • Even though clear or purge may be the recommended solution, it may be more cost effective at times to destroy media rather than use one of these other options • Applied sanitization level can always be increased if it is reasonable and indicated by an assessment of the existing risk so that proper sanitization techniques are applied • NIST publication 800-88 titled “Guidelines for Media Sanitization” provides additional information on sanitization methods and processes.

5.5.4 Dispose of Hardware and Software

Activities:	Hardware and software can be sold, given away, or discarded as provided by applicable regulation. The disposal of software should comply with license or other agreements with the developer and regulations. There is rarely a need to destroy hardware except for some storage media that contains confidential data and that cannot be sanitized without destruction. In situations when the storage media cannot be sanitized appropriately, removal and physical destruction of the media may be possible so that the remaining hardware may be disposed of appropriately. Some systems may contain confidential data after the storage media is removed; if there is doubt as to whether confidential data remains on a system, the Data Steward and Custodian should be consulted before disposing of the system.
Outputs:	Disposition records for hardware and software including but not limited to lists of hardware and software released (sold, discarded, or donated), and lists of hardware and software redeployed to other projects or tasks within the organization.
Synchronization:	Updating of system and component inventories.
Interdependencies:	System hardware and software inventories should be updated accordingly.
Guidance:	• For cost savings, some agencies maintain reasonably old parts for contingency operations. For example, utilizing retired laptops for a telecommuting scenario that requires only partial processing for vital Internet or email communications • A formal process shall be implemented for the authorization of the removal of equipment from a state operated facility or vendor. Removal shall be requested in writing and authorized. Any exceptions to this requirement shall also be in writing.

-- Remainder of Page Intentionally Left Blank –

5.5.5 Closure of System

Activities:	The system is formally shut down and disassembled at this point.
Outputs:	Documentation verifying system closure, including final closure notification to the sponsoring executive management, configuration management, system owner, Data Steward and Custodian, and program manager.
Synchronization:	None
Interdependencies:	• Archival of security documentation as appropriate • If continuous monitoring services are provided, notification to providers of closure is needed (e.g. change configuration groups) • Inventory updates
Guidance:	A memorandum articulating formal system closure and proper action taken that includes in the distribution to all key stakeholders provides the simplest approach to formal closure.

5.6 Legacy System Considerations

In many cases, Divisions and Offices will be applying information security life cycle considerations to legacy information systems that have been in operation for some extended period of time. Some legacy systems may have excellent Security Plans that provide comprehensive documentation of the risk management decisions that have been made, including identifying the security controls currently employed. Other legacy systems may have limited documentation available. The security considerations, however, are still relevant to these legacy systems, and shall be applied and documented to ensure security controls are in place and functioning effectively to provide adequate protections for the system and the associated data.

-- Remainder of Page Intentionally Left Blank –

CHAPTER 6: RISK MANAGEMENT

Managing risk is a complex, multifaceted activity that requires the involvement all organization levels. Executive management must provide the strategic vision with top-level goals and objectives, while mid-level business leaders plan, execute, and manage projects which are implemented by individuals performing system operations that support mission and business functions.

Risk management should be carried out in an holistic manner that encompasses risk from the strategic to the tactical level, ensuring that risk considerations are integrated into every aspect of security decision making with the goal of continuously improving risk related activities, developing effective communication among all stakeholders, and creating a shared interest in the mission/business success of the organization.

Just as with other aspects of security, the goal of risk management should be cost-effective implementation that meets the requirements for protection of an organization's information assets. In each situation, a balance should exist between the system security benefits to mission performance and the risks associated with operation of the system.

Guidelines

Divisions and Offices must create comprehensive operational risk management process(es) that at a minimum address the following four (4) components: (I) frame risk (i.e., establish the context for risk-based decisions), (II) assess risk, (III) respond to risk (once determined), (IV) monitor risk on an ongoing basis using effective communications and a feedback loop for continuous improvement in risk-related activities. Such processes will complement the system security risk assessment at the Department business level (see 6.2.1 System Security Risk Assessment). These four components are detailed below.

A reassessment of risk must be completed any time operations and systems deploy new services, safeguards or as required by the SDLC/PLC (see Chapter 5.0 Life Cycle Security Management).

6.1 Framing Risk

Risk framing establishes the context and common perspective on how risk will be managed in the form of a risk management strategy. Risk framing is based off of a set of assumptions, constraints, risk tolerances, and priorities/trade-offs that shape the organization's approach for managing risk. Risk framing is defined by governance structures, financial posture, regulatory requirements, Department culture, and established relationships (both trusted and untrusted).

Inputs

Inputs to the risk framing component include but are not limited to policies, directives, regulatory compliance requirements, financial limitations which impose constraints on potential risk decisions, identification of trust relationships derived from existing contractual relationships (e.g. Memoranda of Understanding/Agreement (MOU/MOA)), and the identification of limits on decision making authority delegated to business owners for risk decisions. The key precondition for risk framing is executive leadership commitment to defining an explicit risk management strategy and holding business owners responsible and accountable for implementing the strategy.

Because risk strategies defined during risk framing may be inappropriate to some business functions, and the potential for risks to change over time, the risk management process should allow for feedback to the risk framing component from the other three (3) risk process components, as follows:

- Risk assessment: Information generated during the risk assessment may influence the original assumptions, change the constraints regarding appropriate risk responses, identify additional tradeoffs, or shift priorities (e.g. threat/vulnerability information that is useful for one business function could, in fact, be useful for others)
- Risk response: Information uncovered during the development of alternative courses of action could reveal that the risk framing process has failed to uncover some potentially high-payoff alternatives from consideration, thus challenging Divisions and Offices to revisit original assumptions or investigate ways to change the established constraints
- Risk monitoring: Security control monitoring could reveal a class of controls, or a specific implementation of a control, that is relatively ineffective, given the investment requirements in people, processes, or technology, thus leading to changes in assumptions about which types of risk responses are preferred or reconsideration in the risk tolerance level to match operational realities

Tasks

- Risk Assumptions: Identify assumptions that affect how risk is assessed, responded to, and monitored within the organization
- Risk Constraints: Identify constraints on the conduct of risk assessment, risk response, and risk monitoring activities within the organization
- Risk Tolerance: Identify the level of risk tolerance (i.e., willingness to accept or avoid risk) for the organization
- Priorities and Trade-offs: Identify priorities and trade-offs considered by the organization in managing risk

Outputs

The principal output of risk framing is an identified and documented Risk Management Strategy that details how operational risk will be assessed, responded to, and monitored over time, thus making explicit the specific assumptions, constraints, risk tolerances, and priorities/trade-offs used for making operational decisions. In addition, risk framing should produce a set of policies, procedures, standards, guidance, and resources covering the following topics: (I) scope of the operational risk management process (e.g. entities covered, business functions affected, and how risk management activities are applied within the risk management tiers), (II) risk assessment guidance such as characterization of threat sources, information and events, when to consider and how to evaluate threats, risk assessment methodologies, risk assumptions, and the incorporation of the system security risk assessment, (III) risk response guidance such as risk tolerances, risk response concepts to be employed, opportunity costs, trade-offs, consequences of responses, hierarchy of authorities, and priorities, (IV) risk monitoring guidance such as analysis of monitored risk factors to determine changes in risk and monitoring frequency, methods, and reporting, (V) other constraints on executing risk management activities, and (VI) Department priorities and trade-offs.

Outputs from risk framing serve as inputs to the risk assessment, risk response, and risk monitoring components.

6.2 Assessing Risk

The purpose of the risk assessment component is to inform decision makers and identify (I) threats to operations, assets, or individuals, (II) vulnerabilities both internal and external, (III) the harm (i.e., adverse impact) that may occur given the potential for threats exploiting vulnerabilities, and (IV) the likelihood that harm will occur. The end result is a determination of risk (i.e., typically a function of the degree of harm and likelihood of harm occurring).

Inputs

Inputs to the risk assessment component from risk framing include (I) acceptable risk assessment methodologies, (II) the breadth and depth of analyses employed during risk assessments, (III) the level of granularity required for describing threats, (IV) how to assess external service providers, and (V) how to aggregate risk assessment results from different entities or business functions.

Risk assumptions, risk constraints, risk tolerance, and priorities/tradeoffs defined during risk framing shape how risk assessment processes are utilized.

The risk assessment component can also receive inputs from the risk response step (e.g. when the risks of employing new technology-based solutions as alternatives for risk reduction measures are being considered). As courses of action are developed during the risk response component, a differential risk assessment may be needed to evaluate differences that each course of action makes in the overall risk determination.

Tasks

- Threat and Vulnerability Identification: Identify threats to and vulnerabilities in Department information systems and the environments in which the systems operate
- Risk Determination: Determine the risk to Department operations and assets, individuals, other Divisions and Offices, and the nation if identified threats exploit identified vulnerabilities

Outputs

The output of the risk assessment component is a determination of risk to operations (i.e., business, services, regulatory compliance, and reputation), systems, assets, individuals, and other Divisions and Offices.

In certain situations, there are recurring cycles between the risk assessment step and the risk response step until particular objectives are achieved. Based on the course of action selected during the risk response step, some residual risk may remain. Under certain circumstances, the level of residual risk could trigger a reassessment of risk. This reassessment is typically incremental (assessing only the new information) and differential (assessing how the new information changes the overall risk determination).

Outputs from the risk assessment step can be useful inputs to the risk framing (e.g. determinations can result in revisiting the Department risk tolerance) and risk monitoring steps (e.g. risk assessments can include recommendations to monitor specific elements of risk), while particular thresholds established as part of risk monitoring programs can also serve as the basis for reassessments of risk.

6.2.1 System Security Risk Assessment

Divisions and Offices are required to adequately mitigate risks arising from use of data and systems in the execution of missions and business functions. To assist in making the appropriate selection of security controls for systems, the department has adopted the concept of baseline controls. Baseline controls are the starting point for security control and are chosen based on the security category and associated impact levels. The System Security Risk Assessment provides a comprehensive catalog of security controls for systems, arranged by control families and listed by baseline.

Three sets of baseline controls have been identified corresponding to the low-impact, moderate-impact, and high-impact systems. The System Security Risk Assessment describes the process of selecting and specifying security controls and control enhancements for Department information systems to include (I) selecting appropriate security control baselines, (II) tailoring the baselines, and (III) documenting the security controls with defined risk responses based on specialized missions, business functions, and environments of operation.

6.3 Respond to Identified Risk

Once risk has been determined through the risk assessment phase an appropriate risk response that provides a consistent response to risk in accordance within identified risk timeframes must be determined by (I) developing alternative courses of action for responding to risk, (II) evaluating the alternative courses of action, (III) determining appropriate courses of action consistent with defined risk tolerance level, and (IV) implementing risk responses based on the selected courses of action (i.e., a time-phased or situation-dependent combination of risk mitigations, avoidance or transfers).

Inputs

Risk response receives input from both the risk assessment and risk framing components include; (I) identification of threat sources and events, (II) identification of vulnerabilities that are subject to exploitation, (III) estimates of potential consequences or impact if threats exploit vulnerabilities, (IV) estimations of the likelihood that threats will exploit vulnerabilities, (V) a determination of risk to business operations (i.e., financial, regulatory, service, reputation), assets, individuals, other Divisions and Offices (including the department), (VI) risk response guidance from the risk management strategy, and (VII) general executive direction and guidance on appropriate responses to risk.

In addition to the risk assessment and risk framing, risk response can receive inputs from the risk monitoring step (e.g. when Divisions and Offices experience a breach or compromise to their information systems or environments of operation that require an immediate response to address the incident and reduce additional risk that results from the event).

Tasks

- Risk Response Identification: Identify alternative courses of action (i.e., mitigation, acceptance, avoidance or transfer) to respond to risk determined during the risk assessment
- Evaluation of Alternatives: Evaluate alternative courses of action for responding to risk

- Risk Response Decision: Decide on the appropriate course of action for responding to risk
- Risk Response Implementation: Implement the course of action selected to respond to risk

Outputs

The risk response component output is the implementation of the selected courses of action with consideration for (I) individuals or business elements responsible for the selected risk response measures and specifications of effectiveness criteria (i.e., articulation of indicators and thresholds against which the effectiveness of risk response measures can be judged), (II) dependencies of each selected risk response measure on other risk response measures, (III) dependencies of selected risk response measures on other factors (e.g. the implementation of other planned information technology measures), (IV) timeline for implementation of risk response measures, (V) plans for monitoring the effectiveness of risk response measures, (VI) identification of risk monitoring triggers, and (VII) interim risk response measures selected for implementation, if appropriate. There are also ongoing communications and the sharing of risk-related information with elements (i.e., individuals or services) impacted by the risk responses (including potential actions that may need to be taken by the elements).

In addition to the risk monitoring step, outputs from risk response can be useful inputs to risk framing and risk assessment components (e.g. appropriate actions taken during risk response are used to revisit the risk framing component and its associated risk management strategy).

6.3.1 Plan of Action and Milestones

To facilitate a prioritized approach to risk mitigation that is consistent across the system and takes into account vulnerabilities, available resources and realistic strategies for addressing risk, Divisions and Offices must develop and implement a plan of action and milestones that are based on:

- The security categorization of the system
- The specific security control weaknesses or deficiencies
- The proposed risk mitigation approach to address the identified weaknesses or deficiencies in the security controls (e.g. prioritization of risk mitigation actions, allocation of risk mitigation resources)

6.3.2 Risk Assessment Supplemental Information

The PSO will not validate remediation of the gaps identified in the Plan of Action and Milestone (POA&M) report. It is the responsibility of each gap owner (i.e., stakeholder who has ability and authority to remediate an identified gap) to ensure that gaps are being remediated in the time period identified in the POAM. Furthermore, each gap owner should maintain all of the evidence (e.g., exception request approvals or non-approvals, policies, procedures, applicable emails, documentation, etc.) related to the remediation of each gap.

If Risk Assessment deliverables are not received in a timely fashion, the PSO will escalate this non-receipt to the Deputy Secretary, Division Director, and Department Chief Information Officer. Deliverables include, but are not limited to:

- Risk Assessment templates
- Executive Summaries
- POAMs

In order to support the Risk Assessment process, at any time, ISOs and Privacy Officials shall notify the PSO if the HIPAA Coverage determination status changes. Such status changes may result from, but not be limited to the following: Business Associate relationship changes, either internally or externally to the Department, or due to changes in treatment, payment, and operation requirements.

6.3.3 Risk Response Time Frames

Risks identified during the risk assessment process must have an identified response, documented decision and estimated implementation within the time frame appropriate to the risk rating.

- Critical - mitigated within seven (7) days and remediated within twenty-one (21) days

- High - mitigated or remediated within thirty (30) days
- Medium - mitigated or remediated within sixty (60) days
- Low - mitigated or remediated within ninety (90) days

6.4 Monitor Risk

The purpose of the risk monitoring component is to (I) verify compliance, (II) determine the ongoing effectiveness of risk response measures, and (III) identify risk-impacting changes to systems and environments of operation. Analyzing monitoring results allows for the capability to maintain awareness of the risk being incurred, highlight the need to revisit other steps in the risk management process, and initiate process improvement activities as needed. The risk monitoring component must be performed by ISOs and Privacy Officials, with other stakeholders as necessary.

Inputs

Inputs to this step include implementation strategies for selected courses of action for risk responses and the actual implementation of selected courses of action. In addition to these, risk monitoring can receive inputs from risk framing through shaping the resource constraints associated with establishing and implementing an organization-wide monitoring strategy. In some instances, outputs from the risk assessment step may be useful inputs to the risk monitoring step.

Tasks

- Risk Monitoring Strategy: Develop a risk monitoring strategy for the organization that includes the purpose, type, and frequency of monitoring activities
- Risk Monitoring: Monitor Department information systems and environments of operation on an ongoing basis to verify compliance, determine the effectiveness of risk response measures, and identify changes

Outputs

The output from the risk monitoring step is the information generated by (I) verifying that planned risk responses are implemented, security requirements derived from and linked to business functions, and regulatory compliancy requirements are satisfied, (II) determining the ongoing effectiveness of risk responses (consistent with the established risk frame), and (III) identifying risk impacting changes to systems and the environments in which they operate.

Outputs from risk monitoring can be useful inputs to risk framing, risk assessment, and risk response (e.g. compliance monitoring results may require that Divisions and Offices revisit the implementation portion of the risk response step, while effectiveness monitoring results may require that Divisions and Offices revisit the entire risk response step).

6.4.1 Continuous Risk Monitoring Strategy

A critical aspect of managing risks to data from the operation and use of systems involves the continuous monitoring of the security controls employed within or inherited by the system (i.e., conducting a thorough point-in-time assessment of the deployed security controls is necessary but not a sufficient condition to demonstrate security due diligence). The objective of the continuous monitoring strategy is to determine if the implemented security controls continue to be effective in light of the inevitable changes that occur to hardware, software, firmware or the operational environment.

Divisions and Offices must develop and implement a strategy for the continuous monitoring of security control effectiveness including the potential need to change or supplement the control set, taking into account any proposed/actual changes to systems or their environment of operation.

The monitoring of security controls and changes to the system or its operating environment shall be integrated throughout the documented SDLC/PLC processes, as part of a continuous monitoring strategy, and will require the active involvement of system owners and common control providers, IT management, security officers, and authorizing executives. The monitoring strategy will allow for Divisions and Offices to track the security state of systems on a continuous basis and maintain the security authorization for the system over time in dynamic environments of operation with changing threats, vulnerabilities, technologies, and business processes.

An effective continuous monitoring strategy includes but is not limited to:

- Configuration management and control processes for systems
- Security impact analyses on proposed or actual changes to Department information systems and environments of operation
- Assessment of selected security controls (including system-specific, hybrid, and common controls) based on the defined continuous monitoring strategy
- Security status reporting to appropriate individuals (i.e., DHHS PSO, system owner/administrators, Data Stewards and Custodians)
- Active involvement by authorizing executives in the ongoing management of system-related security risks
- The results of continuous monitoring will be incorporated into any necessary updates to the security plan, assessment reports, and plans of action and milestones, as necessary

Guidelines

Where possible, Divisions and Offices should leverage automated tools to facilitate near real-time risk management of information systems. In addition, Divisions and Offices are encouraged to consolidate data to allow for trending analyses and reporting to assist decision makers with timely review and decision making.

Selection of Security Controls for Monitoring

The criteria for selecting which security controls to monitor and for determining the frequency of such monitoring are established in collaboration with system stakeholders (i.e., system owner, security official, Data Steward and Custodian, DHHS P SO, etc.).

Priority for security control monitoring is given to the controls that have the greatest volatility (i.e., a measure of how frequently a control is likely to change over time subsequent to its implementation) and the controls that have been identified in the organization's plans of action and milestones due to the fact that these controls have been deemed to be ineffective to some degree. Consideration for specific threat information including known attack vectors (i.e., specific vulnerabilities exploited by threat sources) when selecting the security controls to monitor and the frequency of such monitoring.

Guidelines

Divisions and Offices should leverage the Priority Code (i.e., P1, P2, P3) assigned to security controls as part of the System Security Risk Assessment. The Priority Codes serve as a recommended sequencing prioritization to help ensure that foundational security controls upon which other controls depend are implemented first, enabling controls to be deployed in a more structured and timely manner in accordance with available resources and providing assistance in level of effort estimations.

6.5 Vulnerability Management

Vulnerability management in practice is designed to reduce the exploitation of system vulnerabilities, both known and unknown (i.e., zero-day exploits) by threats, and is critical to maintaining the operational confidentiality, integrity, and availability of departmental data. The proactive management of vulnerabilities will reduce, and may eliminate, the potential for exploitation resulting in a reduction in time, money and effort involved rather than similar investments after exploitation has occurred.

The DHHS PSO will distribute alerts for common system and service (e.g. Windows OS, Apache, SQL, Adobe Reader, Internet Explorer, Firefox, Chrome, Java, etc.) security related vulnerabilities. Alerts will be classified according to criticality (i.e., Critical, High, Medium, and Low) and distributed to organization Information Security Officials (ISO) and network administrators via email distribution lists. In instances where no known solution(s) (i.e., patches) exist for identified vulnerabilities, the DHHS PSO may take mitigating actions including but not limited to blocking specific services or ports at the department's network perimeter to protect departmental data and systems.

Divisions and Offices must develop comprehensive and repeatable vulnerability management processes, including security patch management and vulnerability remediation, that comply with requirements set forth in the Statewide Security Manual Chapter 4, Section 0201 Technical Vulnerability Management, and has identified metrics for the tracking of vulnerabilities (e.g. Mitigation Response Time, Number of Patches and Vulnerabilities).

Vulnerability findings, either derived from the Department, State or third-party assessments, will be provided by the PSO to each division's ISO and/or Privacy Official. It is the responsibility of the ISO and/or Privacy Official to monitor and track the remediation process with the business owner of the affected system or application and request the PSO to validate the remediation of any vulnerabilities remaining. However, it is the responsibility of each vulnerability gap owner (i.e., stakeholder who has ability and authority to remediate an identified gap) to ensure that such gaps are being remediated appropriately.

Furthermore, each gap owner should maintain all evidence (e.g., exception request approvals or non-approvals, policies, procedures, applicable emails, documentation, etc.) related to the remediation of each vulnerability gap. Remediation of all vulnerabilities must follow risk response times for their severity set forth in section 6.3.3 of this DHHS Security Manual. If vulnerabilities are not remediated within the required response time, the ISO and/or Privacy Official should escalate to their Division Director and Deputy Secretary and notify the Department Chief Information Officer of the escalation. Where any of the security findings are unable to be remediated, a formal exception will need to be filed. The ISO and/or Privacy Official will need to work with the system owner to request an exception through DHHS.SecurityExceptions@dhhs.nc.gov.

Note: Only findings that violate State Standards may have exceptions. Inclusion of any compensating controls, which may act as remediation of risk, will assist in the exception process.

Division ISOs and/or Privacy Officials responsible for these tasks can request from the PSO a copy of the *DHHS Privacy and Security Office Vulnerability Scanning Methodology and Standard Operating Procedures,* which provides additional details regarding ISO and/or Privacy Officials responsibilities in monitoring reported vulnerabilities.

6.6 Security-Focused Configuration Management (SecCM)

Divisions and Offices and systems that have documented standards, procedures and guidelines for Configuration Management (CM) must include security in current processes. In Divisions and Offices and systems that have no existing CM process in place, SecCM practices must be defined from process inception. SecCM is the management and control of secure configurations for a system with the intent to enable security and facilitate the management of risk. SecCM builds on the general concepts, processes, and activities of configuration management and is not meant to stand on its own. SecCM activities include:

- Identification and recording of configurations that impact the security posture of the system and the organization
- The consideration of security risks in approving the initial configuration
- The analysis of security implications of changes to system configurations
- Documentation of the approved/implemented changes

Guidelines

Documenting system changes as part of routine SDLC processes and assessing the potential impact those changes may have on the security state of the system is an essential aspect of vulnerability management, continuous monitoring, maintaining the current authorization, and supporting a decision for reauthorization when appropriate.

6.7 Risk Acceptance

At some point, acceptability of system operation given the type and severity of residual risk must be addressed. Executive management, system owners, Data Stewards and Custodians must fully understand the identified risk in order to make informed decisions. Divisions and Offices typically make determinations regarding the general level of acceptable risk and the types of acceptable risk with consideration of Department priorities and trade-offs between: (i) near-term mission/business needs and potential for longer-term mission/business impacts; and (ii) Department interests and the potential impacts on individuals, other Divisions and Offices, and the State.

Risk acceptance, like the selection of safeguards, should take into account various factors besides those addressed in the risk assessment (e.g. safeguards costs, efforts and resource requirements). In addition, risk acceptance should take into consideration the limitations of the risk assessment (i.e., in some instances risk assessments may rely on speculation, best guesses or incomplete data).

In the event that an identified risk, residual or otherwise, cannot be remediated, Divisions and Offices must formally document the acceptance of the risk. Divisions and Offices may request exception forms by submitting a request to DHHS.SecurityExceptions@dhhs.nc.gov. Exception requests can be made for only North Carolina (NC) Statewide required security standard controls. Findings for Federal systems or data (e.g., HIPAA, IRS, SSA, etc.) must be remediated; risk acceptance is not available.

Guidelines

Department documents for the acceptance of risk must rate the risk as low, moderate, or high describe in detail the justification for the rating based on the particular situation(s) or condition(s).

All risk acceptances should be reviewed bi-annually at a minimum or as system changes require.

CHAPTER 7: DATA SECURITY ENHANCEMENTS

7.1 Security Plan Development

Security Plans provide an overview of the security requirements for systems within an organization and describe the security controls in place, or planned, for meeting those requirements. The plans also describe the rationale for security categorization, tailoring, and supplementation activities, how individual controls are implemented within specific operational environments, and any usage restrictions to be enforced on systems due to high-risk situations. Security Plans are important because they document the decisions taken during the security control selection process and the rationale for those decisions. System Security Plans shall include at a minimum:

- The security categorization of the system including supporting rationale
- Full descriptive name of the information system including associated acronym
- Unique information system identifier (typically a number or code)
- System owner, Data Steward/Custodian, and authorizing official including contact information
- Information on the organization(s) that manages, owns and controls the system
- Location of the system and environment in which it operates
- Version or release number of the system
- Purpose, functions, and capabilities of the system and details of the essential functions or business processes supported • Technical security architecture
- Status of the system with respect to acquisition or life cycle
- Applicable laws, directives, policies, regulations, or standards affecting the security of the system
- Describes the security controls in place or planned for meeting data security requirements including a rationale for the tailoring and supplementation decisions
- Types of data processed, stored, and transmitted by the system
- Boundary of the system for risk management and security authorization purposes
- Architectural description of the system including network topology
- Hardware and firmware devices included within the system
- System and applications software resident on the system
- Hardware, software, and system interfaces (internal and external)
- Subsystems (static and dynamic) associated with the system
- Data flows and paths (including inputs and outputs) within the system
- Cross domain devices/requirements
- Network connection rules for communicating with systems (both internal and external)
- Interconnected systems and identifiers for those systems

- Encryption techniques used for information processing, transmission, and storage[3]
- Cryptographic key management information (e.g. public key infrastructures, certificate authorities, etc.)
- System user types including Department affiliations, access rights, privileges, citizenship (if applicable)
- Ownership/operation of system (e.g. government-owned, government-operated; government-owned, contractor operated; contractor-owned, contractor-operated; nonfederal [state and local governments, grantees])
- Security authorization date and authorization termination date
- Incident response outline with points of contact
- Other information as required by the organization
- Site Security Plan (SSP) as required

They are approved by appropriate authorizing officials within the organization and provide one of the key documents in security accreditation packages that are instrumental in authorization decisions.

Updates to the security plan may be triggered by a variety of events, including: (I) vulnerability scan or assessment of the system or operating environment, (II) new threat information, (III) weaknesses or deficiencies discovered in currently deployed security controls after an system breach, (IV) a redefinition of essential functions, priorities or business objectives invalidating the results of the previous security categorization process, and (V) a change in the information system (e.g. adding new hardware, software, or firmware or establishing new connections) or its environment of operation (e.g. moving to a new facility).

Guidelines

NIST Special Publication 800-18 provides guidance and can serve as a basis for the development of the system security plan.

7.2 Media Security

Divisions and Offices must develop and implement processes for the safeguarding and control of data on Portable Electronic Devices (PED) and removable media based on risks identified through risk management (see Chapter 6: Risk Management). The processes shall include handling and usage requirements for PEDs and removable media during the transportation, processing or storage of confidential data, prohibiting access by unauthorized persons to devices and media when not in use and guidelines for connecting to devices and media to non-Department systems or networks.

Guidelines

Divisions and Offices should consider implementing PED and removable-media disposal procedures that require workforce members to drop off old or nonfunctioning devices in secured containers or with an identified individual for periodic and proper destruction.

7.2.1 Remote Access

Divisions and Offices must ensure its authorized users of DHHS computer systems, state network, and data repositories are permitted to remotely connect to those systems for the sole purpose of conducting DHHS related business. For purposes of this manual and in accordance with the NC DIT State Information Security Manual, **Remote Access** shall mean the ability of a resource to access the state's network via an external network connection. Remote access generally occurs from remote locations such as homes, hotel rooms, and off-site offices. Remote connections shall be accessed only through a secured, authenticated, and protected access method. At a minimum, the following remote user access guidance shall be implemented:

- Authentication and authorization systems for remote access shall be managed by the Divisions and Offices using the North Carolina Identity Management Service (NCID).
- Multifactor Authentication (MFA) must be used for remote access to all applications.

[3]. NIST publication 800-52r1 titled "Guidelines for the Selection, Configuration, and Use of Transport Layer Security (TLS) Implementations" provides additional information on encryption of data in transit. NIST publication 800-111 titled "Guide to Storage Encryption Technologies for End User Devices" provides additional information on the encryption of data at rest.

- Revocation/Modification of remote access shall occur at any time for reasons including noncompliance with security policies, request by the user's supervisor, the Division Information Security Official (ISO), or if there is a negative impact on overall network performance attributable to remote connections.
- There shall be certain remote access users who warrant use of file and/or disk encryption technology. This shall be based on whether confidential records are included in the information that they are able to store on their local systems.
- Audit logs of remote access activities shall be maintained for at least ninety (90) days.

Guidelines

Divisions and Offices shall ensure than remote access to any DHHS resource from an external or non-state source must originate through a virtual private network (VPN). Any other remote access utilities must have specific authorization from the Division Information Security Official (ISO) for their use.

7.3 Cloud Security

Divisions and Offices looking to leverage the many benefits, innovations and practicable efficiencies promoted by cloud computing (e.g. on-demand delivery of applications, self-service, ability to scale up or down, and usage-based economics) must ensure the application of appropriate security controls and risk responses. Common cloud services and technologies include but are not limited to:

- Infrastructure as a service (IaaS)
- Platform as a service (PaaS)
- Software as a service (SaaS)
- Test environment as a service (TEaaS)
- Desktop virtualization

While cloud computing can be implemented exclusively for an organization (i.e., private cloud), often it is utilized as a means to outsource parts of the Department computing needs (i.e., public cloud or outsourced private cloud). As with any outsourcing of information technology services, concerns exist about the implications for data security. One of the main issues centers on the risks associated with moving applications, infrastructure, services or data from within the confines of the organization's environment to that of another's (i.e., the cloud provider).

Guidelines

Because cloud computing brings its own set of security challenges, it is essential for an organization to oversee and manage how the chosen cloud deployment model (i.e., public, private, community and hybrid) secures and maintains data, and compliance including meeting applicable regulations, data location and electronic discovery requirements.

7.4 Social Media Security

Divisions and Offices must the assess risk (see Chapter 6: Risk Management) associated with the use of social media sites (e.g. Facebook, Twitter, and LinkedIn etc.) in the conduct of business activities. These sites allow for communities of individuals with common interests to communicate, share and exchange feedback pertaining to those interests. Social media sites typically leverage customized tools in web-based environments that promote collaborative communication and dissemination of information. Social media can be either managed in-house (i.e., self-hosted) or externally hosted either as a paid hosting service or as part of a cloud hosted solution.

Once Divisions and Offices have decided on how particular social media technologies will be leveraged, they must:

Develop a Social Media Rules of Behavior policy on the purpose and appropriate use of the social networking site by Department workforce that provides guidance to workforce members and complies with Departmental and Statewide Privacy and Security Standards, The rules should also be in compliance with Best Practices for State Agency Social Media Usage in North Carolina.

- Identify workforce members who are authorized to maintain social media sites on behalf of the organization, and provide guidance to authorized personnel on the use and maintenance of social media used in connection with Department business

- Train users on appropriate practices for use of social networking sites including the Social Media Rules of Behavior policy
- Routinely monitor workforce access and use of identified social media sites
- Institute data safeguards and risk response appropriately for the preservation and prevention of loss of Department data
- Document the identified social media usage in appropriate security documentation (e.g. security plans, continuity plans, training material, etc.)
- Ensure the chosen social media meets all required regulatory compliance

Guidelines

Social media sites can serve as valuable outlets for Department outreach efforts in times of crisis and disaster; Divisions and Offices should consider leveraging social media with regards to continuity planning efforts (see Chapter 8: Continuity of Operations Planning).

7.5 Security Assessments and Monitoring

An information security assessment is the process of determining how effectively an entity being assessed (e.g. host, system, network, procedure, person—known as the assessment object) meets specific security objectives. Four (4) types of assessment methods can be used to accomplish this:

- Examination is the process of checking, inspecting, reviewing, observing, studying, or analyzing one or more defined objects to facilitate understanding, achieve clarification, or obtain evidence
- Interviewing is the process of conducting discussions with individuals or groups within an organization to facilitate understanding, achieve clarification, or identify the location of evidence
- Functional testing is the process of exercising one or more defined objects under specified conditions to compare actual and expected behaviors (see 5.2.5)
- Technical testing used to identify, validate, and assess technical vulnerabilities to assist in understanding and improving network or system security posture

Divisions and Offices are granted the authority to perform security assessments by means of examination, interviewing and functional testing only. In instances where technical testing is required, Divisions and Offices shall contact the DHHS PSO requesting technical security testing.

Department workforce members shall not download, install or run security programs or utilities that reveal weaknesses in Department networks and systems or reveal identifiable or confidential data, both in transit and at rest, without prior written approval from the DHHS Chief Information Security Officer (CISO). Examples of security tools include but are not limited to:

- Password-cracking utilities
- Packet sniffers
- Network-mapping tools
- Port scanners

7.6 Personally Owned Equipment and Software

Divisions and Offices must develop a Bring Your Own Device (BYOD) strategy that includes policies and processes related to the use (i.e., whether allowed or not) of personally owned equipment and software. The goal of a Department BYOD strategy should be to accommodate its workforce's lifestyles and work habits while protecting Department data and infrastructure from risks associated with devices. BYOD strategies must at a minimum consider:

- Education, use, and operation (see 2.7 Information Security Education Training and Awareness (SETA))
    - Ensure consistency with Department requirements standards for processing, transmitting and storing confidential data
    - Establish orientation, training, and user agreements
    - Consider impact of connectivity and data plan needs for of chosen technical approach (e.g. virtualization)
    - Which workforce members will be eligible for BYOD

- Security
    - Ensure consistency with Department requirements standards for processing, transmitting and storing confidential data
    - Assess and document risks in (see Chapter 6: Risk Management):

        Information security (operating system compromise due to malware, device misuse, and information spillover risks);
        Operations security (personal devices may divulge information about a user when conducting specific activities in certain environments);
        Transmission security (protections to mitigate transmission interception).

    - Ensure consistency with Department requirements standards for processing, transmitting and storing confidential data
    - Assess data security with BYOD versus the devices being replaced
    - Securely design/architect systems for interoperability (Department data vs. personal data)
    - Determine security requirements at the device, application, and data access level

- Privacy
    - Identify the right balance between personal privacy and Department security
    - Document process for employee to safeguard personal data if/when the organization wipes the device

- Ethics/legal questions
    - Define “acceptable use” from both Department and individual perspective
    - Address legal discovery (including confiscation rights) and liability issues (e.g. through pre-defined opt-in requirements in terms of service)
    - Consider implications for equal rights employment (e.g. disparity in quality of personal devices)

- Devices and applications (apps)
    - Identify permitted and supported devices to prevent introduction of malicious hardware and firmware
    - Define content applications that are required, allowed, or banned and consider use of mobile device management (MDM) and mobile application management (MAM) enterprise systems to enforce policies
    - Adopt existing app development best practices to support device-agnosticism and data portability across platforms (see Chapter 4.0 System Acquisition, Development and Maintenance)
    - Address app compatibility issues (e.g. accidental sharing of sensitive information due to differences in information display between platforms)
    - Recommend approach to content storage (cloud vs. device)
    - Clarify ownership of the apps and data

- Asset management
    - Disposal of device if replaced, lost, stolen, or sold, or employment is terminated (must remove government information before disposal)
    - Reporting and tracking lost/stolen personal devices
    - Replacement of personal lost devices if employee chooses not to replace with personal funds
    - Identification of boundaries for service and maintenance

Systems and associated equipment (e.g. laptop, smart phone, tablet, flash storage, etc.) that are not owned, leased or operated on behalf of the organization shall not be connected to Department equipment or networks without prior written approval from the organization’s Information Security Official. Additionally, workforce members engaging BYOD must sign an acceptable use policy before connecting personal devices to the corporate network.

Guidelines

Divisions and Offices choosing to support BYOD should consider enforcing encryption of data at rest, workspace or application sandboxing or a combination of technologies to ensure the safeguarding of data.

7.7 Physical Security

Divisions and Offices must conduct risk assessments for workspace environments (e.g. buildings) in order to identify potential threats to workforce members or assets and implement appropriate measures to provide physical security controls for the protection confidential information.

Divisions and Offices must apply the principles of Control, Deter, Detect and Delay/Respond as part of their physical security risk management strategy. Each concept is supported by security components (i.e., physical and technological safeguards, processes and procedures) that deter, detect or support physical security elements. Physical safeguards include but are not limited to: perimeter barriers, surveillance systems, lighting, locks, electronic security systems and protective forces. Many times, a single measure can accomplish more than one of the Control, Deter, Detect and Delay/Respond principles.

- **Control:** This is the ability of an organization to manage its activities and assets. Control requires Divisions and Offices to have defined policies, procedures and technologies in place that establish rights, authorities and responsibilities and to provide monitoring and feedback. A well-designed Control strategy maintains a reporting and management structure, and can supplement or enhance existing data safeguards.

- **Deter:** The perception (i.e., a psychological state) on the part of the threat that the risk or effort required to be successful is greater than that of the payoff. The goal of a successful deterrence strategy is to lead to reluctance on behalf of the potential threat. Deterrence strategies can be enhanced through the provisioning of multiple layers of security (e.g. requiring personnel to pass through several control points to gain facility access).

- **Detect:** This is the ability for Divisions and Offices to identify a threat. Detection is the first step in the response as the sooner threat is detected, the sooner an appropriate response can be initiated. Divisions and Offices must determine how soon and by what means workforce members will be alerted to the detected threat. Where possible, Divisions and Offices should leverage technology to assist in determining the validity of an alarm in preparation for an appropriate response.

- **Delay/Respond:** This is the ability of physical and psychological barriers to restrict movement and prevent a threat from succeeding long enough to allow for an appropriate response (e.g. staff or law enforcement intervention) to be initiated. Often Delay/Response may depend on the implementation of multiple layers of physical security such as a combination of barriers, locks and lighting.

Guidelines

Department workforce members should:

- Be vigilant and report any suspicious activity or individuals (i.e., it's better to be safe than sorry)
- Know their environment (i.e., building, workspace, etc.) and report anything out of place, missing, or items that do not appear to belong
- Understand and actively cooperate with check-in procedures and physical security and visitor policies. In addition to the Statewide Information Security Manual policy (SCIO-SEC-313-00), visitor policies shall include the requirement to ensure visitor records are publicly accessible for a minimum of 2 years
- Share ideas and suggestions about how to enhance workplace security and safety

7.8 Access Controls

In accordance with the NC Statewide Information Security Manual "Access Control" policy, NC DHHS will perform regular access control reporting. Reports will be submitted to the Privacy and Security Office at the end of the month following the quarter. The following schedule shall be used for reporting access reviews within your division/office:

Report Period	Report Due
January, February, March	End of Month (EOM) April (privileged users)
April, May, June	EOM July (ALL USERS)
July, August, September	EOM October (privileged users)
October, November, December	EOM January (All USERS)

7.8.1 Identification and Authentication

NC DHHS Division and Offices information systems shall be configured to uniquely identify and authenticate users or processes. Access to NC DHHS information systems shall be through local or network access. At a minimum, this process shall ensure the following;

- Prohibition of shared accounts
- Information system level and application level mechanisms as determined by a risk assessment; and
- Access to all accounts (local, privileged, non-privileged) shall be authenticated using multifactor authentication (MFA). MFA shall be used under the following conditions:
    - Remote access to information systems using privileged accounts
    - Remote access to information systems using privileged and non-privileged accounts for information systems that receive, process, store, or transmit federal tax information (FTI), personally identifiable information (PII), protected health information (PHI), or other highly confidential data

NC DHHS Division and Offices shall require that all users accessing NC DHHS networks adhere to required security configurations for their devices, including required patches and updated anti-virus signature files. All information systems, including cloud services, shall include the following at a minimum;

- Obtain authorization from the security manager
- Ensure single users or devices have a single unique identifier that identifies an individual, group, role, or device
- Prevent reuse of identifiers for seven (7) years
- Disable identifiers after 120 days of inactivity unless exempted by management
- Delete or archive identifiers that have been disabled for more than 365 days
- Disable accounts within 60 days of inactivity for user and non-user accounts

Guidelines

NC DHHS shall manage information system authentication requirements. Individual authenticators include passwords, tokens, biometrics, PKI certificates, and key cards. NC DHHS shall require the at least the minimum guidelines outlined in the NC DIT Statewide Information Security Manual.

7.9 Capital Planning and Budgeting

Divisions and Offices authorizing officials typically have budgetary oversight for an information system or are responsible for the business operations supported by the system. The authorizing official shall meet the requirements of the North Carolina Office of Budget and Management's information security budgeting policy through their project request process.

CHAPTER 8: CONTINUITY OF OPERATIONS PLANNING (COOP)

Divisions and Offices must develop and maintain continuity plans, processes and procedures that provide the foundation for the continued performance of essential functions under a wide range of circumstances, conditions and potential emergencies. Risk management principles shall be applied to all elements of continuity planning in order to safeguard data and minimize the security impact of uncertain events.

The objectives of a continuity plan include but are not limited to:

- Ensuring the organization can perform its essential functions, if applicable, under all conditions
- Communicating advisories, alerts, and plan activation to employees, with instructions for relocation to pre-designated facilities, with and without warning, during duty and non-duty hours
- Reducing the loss of life and minimizing property damage and loss
- Executing successful orders of succession with accompanying delegation of authorities in the event of a disruption rendering leadership unavailable, or incapable, of assuming and performing their authorities and responsibilities
- Reducing or mitigating disruptions to operations
- Ensuring that the agency has facilities where it can continue to perform its essential functions, as appropriate, during a continuity event
- Protecting personnel, facilities, equipment, records, and other assets, in the event of a disruption
- Achieving a timely and orderly recovery and reconstitution (i.e., transitioning from COOP status back to normal operations) from an emergency
- Ensuring and validating continuity readiness through a dynamic and integrated continuity test, training, and exercise (TT&E) program and operational capability
- Alternative sites (i.e., facilities) for business operations
- Interoperable communications (i.e., the ability for Divisions and Offices including local, state and federal to talk with each other and share data as the situation requires)
- Identifying and documenting vital records (i.e., records vital to sustaining essential functions)
- Managing human capital (i.e., the sum of the competencies individuals invest in their work such as social and personality attributes, knowledge, enthusiasm, and creativity)
- Devolution (i.e., the capability to transfer statutory authority and responsibility for essential functions from a primary operating staff or facilities to others that can sustain operational capability for an extended period)

Continuity planning considerations should include:

- Maintaining a high level of readiness
- Capability of implementation both with and without warning
- Ability to be operational no later than twelve (12) hours after activation
- Maintain sustained operations for up to thirty (30) days
- Taking maximum advantage of existing infrastructures

Divisions and Offices within DHHS are required to submit continuity plans to the DHHS PSO on an annual basis for review, cataloging and storage.

Guidelines

DHHS has adopted the Federal Emergency Management Agency's (FEMA) Continuity Plan Template and Instructions for Non-Federal Entities as the basis for Department COOP documents.

8.1 Business Continuity Planning (BCP)

Within the department BCP is a system-focused plan designed to restore operability of the target system, application, or Information Technology (IT) infrastructure after an emergency. The BCP should support Department continuity plans (i.e., COOP) by recovering supporting systems and infrastructures for essential functions.

Each organization shall designate staff as required to development and participate in the development, testing, training and implementation of organization system specific continuity plans and:

- Evaluate the organization, managerial, and technical environments in which the BCP/DR plan(s) must be implemented
- Identify the types of disruptions most likely to occur and the resultant impacts on the system(s) ability to perform/support essential functions
- Propose protective measures to be implemented in anticipation of a natural or man-made disasters
- Coordinate plan development with other required system stakeholders
- Develop processes for the periodic review and updating of plans for completeness and compliance
- Create and maintain policies and procedures in support of business continuity and recovery efforts
- Design testing/training schedules and strategies to validate the system and business recovery plans

Divisions and Offices shall leverage the State's chosen BCP software, to identify, categorize and document the Disaster Recovery (DR) and continuity planning of IT systems. Plans input into the State's chosen BCP software, shall include:

- Practices that ensure compliance to applicable federal or state legislation, rules or conditions of funding specific to business continuity or disaster recovery
- Identification of workforce roles and responsibilities related to system recovery processes
- A business impact analysis that identifies time sensitive business functions, financial, social, and regulatory impacts • A risk assessment to determine risk priorities and probability of identified risk
- Plan activation and notification procedures
- Communication Plan including crisis communication procedures and coordination with other applicable public authorities
- Emergency response procedures based upon type of emergency(s) and identify command and control procedures for the recovery operation
- Provision for the replacement of data, equipment and staff resources, and inclusion of manual workaround procedures (if possible) in the event of a disruption
- Identification of alternate locations, facilities, off-site storage, critical resources and inventories for plan implementation
- Development of recovery/restoration procedures for time critical system functions

Divisions and Offices within DHHS are required to submit IT continuity plans (i.e., BCP) to the DHHS PSO on an annual basis for review. The DHHS PSO shall submit, on behalf of the department, the BCPs on an annual basis to the State Chief Information Officers Office as required by North Carolina General Statute §147-33.89.

Guidelines

Plans should provide quick and clear directions in the event that personnel unfamiliar with the plan or the systems are called on to perform recovery operations. Plans should be clear, concise, and easy to implement in an emergency, and where possible, checklists and step-by-step procedures should be used.

8.1.1 Identification of Application Criticality

Often during circumstances that require the activation of BCP processes; resources by which Divisions and Offices can contain impacts and recover systems are limited. Divisions and Offices must be able to give clear direction to resources about system recovery priorities, and in order to so must define the relative criticality of the application.

The process is which Divisions and Offices determine the relative criticality of applications should not be laborious but rather simple business decision about where the application falls under the state's four (4) defined criticality ratings, which are:

- **Statewide Critical:** From an information technology perspective, in the agency's opinion, the loss of this application will have a direct impact to statewide core functions, processes or activities. The application's loss may also impact a large portion of the State's population.
- **Department Critical:** From an information technology perspective, in the agency's opinion, the loss of this application will have a direct impact to this department's core functions, processes or activities.
- **Program Critical:** From an information technology perspective, in the agency's opinion, the loss of this application will have a direct impact to the core functions, processes or activities associated with a program within this agency.
- **Non Critical:** From an information technology perspective, in the agency's opinion, the loss of this application will have little or no impact to Statewide, or this department's core functions, processes and activities or the core functions, processes and activities associated with a program within this agency.

Application criticality level must be documented within each application's BCP and should be reviewed annually as part of the continuity planning process to ensure applications continue to meet the defined criticality level.

Guidelines

Application criticality level is not the sole factor in the determination of recovery priority. Recovery priorities are a direct output of the Business Impact Analysis process (Chapter 8.3 Business Impact Analysis) which includes system criticality, which application criticality is a subset of.

8.2 Business Impact Analysis (BIA)

A BIA is designed to predict the consequences (i.e., impacts) of disruptions to business functions and processes, and to assist in gathering information needed to develop recovery priority strategies. Potential loss scenarios should be identified as part of the risk assessment process, and Divisions and Offices should seek to consider as many scenarios as possible during the BIA process.

Through the BIA process Divisions and Offices will identify the sections and processes that are critical to the recovery of essential functions, and Department-wide interrelationships (both functional and system based).

Divisions and Offices shall utilize the DHHS BIA template and upload the completed template to the State's chosen BCP software to correlate the system with the critical business processes and services that conducted in the fulfilling of Department missions and essential functions.

Guidelines

Divisions and Offices should strive to give clear directions, based on priority strategies, to resources involved in Department recovery efforts. This will allow for a criticality analysis yielding different levels of criticality with varying recovery times with the most important information assets being recovered first and least important potentially last.

8.3 Risk Management within Continuity of Operations

Risk management principles shall be applied to all elements of continuity planning. Risk management is the process to identify, control, and minimize the impact of uncertain events. Although there are many well-documented methodologies for risk management - some of these are referred to as risk analysis - most require an assessment and understanding of three basic concepts:

- The consequences of not protecting valuable assets (i.e., people, information, and facilities) and/or not performing essential functions
- The threat environment (as it relates to a particular agency or area of concern)
- The level of vulnerability to the relevant threats

8.3.1 Adherence to Security Controls

The security controls established as part of the System Security Risk Assessment (see 6.2.1) provide a solid baseline foundation for the safeguarding of system data. BCP and COOP documents must appropriately address adherence to identified security controls in

an effort to manage risk and protect DHHS data against threats, both identified and ones that are a result of the disruption, as part of contingency planning.

8.4 Continuity Plan Testing and Training

Divisions and Offices' continuity plans, including BCP, should be maintained in a state of readiness, which includes having personnel trained to fulfill their roles and responsibilities identified within the plan, having plans exercised to validate their content, and having systems and system components tested to ensure their operability in the event of an emergency.

8.4.1 Testing

Divisions and Offices must conduct BCP testing annually, as required by the Statewide Security
Manual Chapter 14, Section 140104 Testing the BCP, to validate that defined business continuity recovery strategies will work. Tests should also be conducted to verify that systems, system components and equipment perform as designed. Testing examples include:

- Tabletop testing or Structured walk-through (i.e., a step-by-step walk-through where the disaster recovery team role-play a disaster scenario prepared by a test moderator)
- Simulations (i.e., advance tabletop, includes business leaders, partners, vendors, management and staff; no technical recovery is done)
- Technical recovery testing (i.e., testing systems in real-life situations ranging from media backup tests to alternative site operational switchovers)
- Testing of hot-site arrangements, complete rehearsal (testing organization, personnel, equipment, facilities and processes)
- Complete rehearsal (i.e., testing organization, personnel, equipment, facilities and processes)

8.4.2 Training

Training for personnel with continuity plan responsibilities should focus on familiarizing them with their assigned roles, teaching skills necessary to accomplish the tasks associated with the roles, and preparing personnel to participate in tests and exercises as well as actual outage events. Personnel newly appointed to continuity roles should receive training shortly thereafter. Recovery personnel should be trained on the following plan elements:

- Purpose of the plan
- Cross-team coordination and communication
- Reporting procedures
- Security requirements
- Team-specific processes (Activation and Notification, Recovery, and Reconstitution Phases)
- Individual responsibilities (Activation and Notification, Recovery, and Reconstitution Phases)

Guidelines

Continuity plan training should be provided to the identified organization personnel annually to enable them to execute their respective recovery roles and responsibilities without aid of the actual continuity documentation.

-- Remainder of Page Intentionally Left Blank --

CHAPTER 9: SYSTEM AUTHORIZATION

System authorization is based on an assessment of management, operational, and technical controls of the system by an authorizing official who is a senior or executive with the authority to formally assume responsibility for operating an information system at an acceptable level of risk to Department operations and assets, individuals, and other Divisions and Offices. Authorizing officials typically have budgetary oversight for an information system or are responsible for the business operations supported by the system.

Authorizing officials also approve security plans, memorandums of agreement or understanding, and plans of action and milestones and determine whether significant changes in the information systems or environments of operation require reauthorization.

In the event that there is a change in authorizing officials during the system authorization process, the new authorizing official reviews the current authorization decision document, authorization package, and any additional documents. If the new authorizing official is willing to accept the currently documented risk, then the official signs a new authorization decision document, thus formally transferring responsibility and accountability for the system or the common controls inherited by the system. If the new authorizing official is not willing to accept the previous authorization results (including identified level of risk), a reauthorization action is required to be initiated in order to establish new terms and conditions for continuing the system's authorization. In instances of reauthorization, the original authorization termination date will be extended for a time not to exceed three (3) years.

Guidelines

Systems completing the State's Project Review Life Cycle (i.e., Project Portfolio Management) shall receive authorization to operate as part of the approval process.

9.1 Authorization Package

The security authorization package documents the results of the security control assessment and provides the authorizing official with essential information needed to make a risk-based decision on whether to authorize operation of a system or a designated set of common controls. The information system owner, who is responsible for the assembly, compilation, and submission of the authorization package, receives inputs from the Data Steward and Custodian, security control assessor, system administrator (as required), and the Information Security Official during the preparation of the authorization package. The authorization package contains the following documents:

- Security plan which provides sufficient information to understand the intended or actual implementation of each security control employed or inherited by the system. The security plan also contains, as supporting appendices or as references to appropriate sources, other risk and security-related documents such as a risk assessment, data impact assessment, system interconnection agreements, contingency plan, security configurations, configuration management plan, incident response plan, and continuous monitoring strategy
- Security assessment report which provides the results of assessing the implementation of the security controls identified in the security plan to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the specified security requirements. The security assessment report also contains a list of recommended corrective actions for any weaknesses or deficiencies identified in the security controls
- Plan of action and milestones which describes the specific measures planned to correct weaknesses or deficiencies noted in the security controls during the assessment, and address known vulnerabilities in the system

After completion of the security plan, security assessment report, and plan of action and milestones, the information system owner submits the final security authorization package to the authorizing official for authorization sign-off.

Guidelines

The documents in the authorization package should be updated accordingly based on actual events that may affect the security state

of the system.

9.2 Authorization Decisions

Authorization decisions are based on the content of the authorization package and any additional supporting documentation required by the authorizing official.

The security authorization package provides comprehensive information on the security state of the system. Inputs, including established risk guidance derived from the risk management strategy, provide additional information to the authorizing official that may be relevant and affect the final authorization decision (e.g. risk tolerance, risk mitigation strategy, business requirements, dependencies among systems, risk monitoring requirements, and other types of risks not directly associated with the system or its environment of operation). Risk inputs are documented as part of the authorization decision. Divisions and Offices must determine, as part of their life cycle security and risk management, how the risk management strategy and related guidance influences authorization decisions. Security authorization decisions are conveyed to the system owner, the DHHS CISO, and selected individuals (e.g. information system owners inheriting common controls, authorizing officials for interconnected systems, information security officials, Data Stewards and Custodians).

In addition, the periodic review of controls should also contribute to future authorizations, with reauthorization occurring whenever there is a significant change in safeguards, data processing, or a three (3) year span of time has occurred. A significant change is defined as a change that is likely to affect the security state of an information system (e.g. modifications to cryptographic modules, security controls or moving to a new facility).

There are two types of authorization decisions that can be rendered by the authorizing official:

- **Authorization to Operate:** If the authorizing official, after reviewing the authorization package, deems that the risk to operations, assets, individuals or other Divisions and Offices is acceptable, an authorization to operate is issued for the system. The system is authorized to operate for a specified time period in accordance with the terms and conditions established by the authorizing official (i.e., the timeframe typically specified with contracts and projects)
- **Denial of Authorization to Operate:** If the authorizing official, after reviewing the authorization package, deems that the risk to operations, assets, individuals or other Divisions and Offices is unacceptable and immediate steps cannot be taken to reduce the risk to an acceptable level, a denial of authorization to operate is issued for the information system or for the common controls inherited by Department information systems

Failure to receive an authorization to operate indicates that there are major weaknesses or deficiencies in the security controls employed within or inherited by the system. The authorizing official or designated representative works with the system owner or common control provider to revise the plan of action and milestones to ensure that appropriate measures are taken to correct the identified weaknesses or deficiencies.

Guidelines

When a formal reauthorization action is initiated, the organization should target only the specific security controls affected by the changes and reuse previous assessment results wherever possible. An effective risk management process that covers all phases of the lifecycle can significantly reduce the overall cost and level of effort of reauthorization actions.

9.2.1 Authorization Rescission

A special case of a denial of authorization to operate is an authorization rescission. Authorizing officials or the DHHS PSO can rescind a previous authorization decision at any time in situations where there is a specific violation of: (I) federal, state or departmental policies, directives, regulations, standards, guidance or practices, or (II) the terms and conditions of the original authorization (e.g. failure to maintain an effective continuous monitoring program may be grounds for rescinding an authorization decision). Authorizing officials and the DHHS PSO must consult with each other prior to rescinding security authorizations.

9.3 Authorization Decision Document

The authorization decision document transmits the final authorization decision from the authorizing official to the information system owner and other key stakeholders, as appropriate. The authorization decision document contains the following information:

- Authorization decision (i.e., authorized to operate or not)
- Terms and conditions for the authorization (i.e., a description of limitations or restrictions placed on the operation of the system or common controls)
- Authorization termination date (i.e., a predetermined time when the security authorization expires, and reauthorization is required; default is three (3) years
- Risk input (if provided)

The authorization decision document is attached to the authorization package and transmitted to the identified stakeholders. The authorizing official verifies on an ongoing basis, that the terms and conditions established as part of the authorization are being followed by the system or common control provider, including the individuals with responsibilities to each.

-- Remainder of Page Intentionally Left Blank --

CHAPTER 10: INCIDENT RESPONSE

To ensure appropriate actions are taken in an effort to minimize loss, Divisions and Offices must develop internal processes to respond quickly and efficiently when significant cybersecurity incidents or breaches occur including:

- Identifying individuals that will assist in the DHHS Privacy and Security Office with incident response and reporting
- Developing procedures to assist in identifying and reporting significant cybersecurity incidents in a timely manner
- Documenting incidents with as much detail as possible (e.g. describe the incident, time discovered, who was notified and what actions were taken, impacted area, etc.)
- Assess and take appropriate incident mitigation and remediation steps (i.e., applying patches, blocking network traffic, deactivation of accounts, etc.)
- Respond to incidents (i.e., work with the DHHS PSO to contain, investigate and resolve significant cybersecurity incidents)
- Determine incident impact to systems, services, operations and data
- Conduct postmortems (i.e., lessons learned) in order to identify and make changes that improve the incident response process
- Securely retaining logs and corresponding incident documentation for a minimum of one (1) year following the discovery of an incident or until all investigations are completed
- Interoperability of incident response and continuity planning for incidents that impact the safety of citizens, personnel, facilities or results in a situation where agency services are interrupted for an extended period of time

Guidelines

A Significant Cybersecurity incident, previously termed "Security Incident", is a cybersecurity incident that is likely to result in demonstrable harm to the State's security interests, economy, critical infrastructure, or to the public confidence, civil liberties, o public health and safety of the residents of North Carolina. A significant cybersecurity incident is determined by the following factors:

- Incidents that meet thresholds identified by the Department jointly with the Department of Public Safety that involve information:
    - That is not releasable to the public and that is restricted or highly restricted according to Statewide Data Classification and Handling Policy; or
    - That involves the exfiltration, modification, deletion, or unauthorized access, or lack of availability to information or systems within certain parameters to include (i) a specific threshold of number of records or users affected as defined in G.S. 75-65 or (ii) any additional data types with required security controls.

Incidents that involve information that is not recoverable or cannot be recovered within defined time lines required to meet operational commitments defined jointly by the State agency and the Department or can be recovered only through additional measures and has a high or medium functional impact to the mission of an agency. In instances where significant cybersecurity incidents occur across Department or network boundaries, the DHHS PSO shall define the protocols for handling these incidents and coordinate communications between required Divisions and Offices.

10.1 Incident Reporting

All significant cybersecurity incidents classified as level 3, 4, or 5 must be reported to the DHHS PSO and the organization Information Security Official within a period of 24 hours from the time the incident was discovered. Incidents reported to the DHHS PSO shall be done through the incident reporting web portal at https://www.ncdhhs.gov/about/administrative-divisions-offices/office-privacy-security. Reporting of significant cybersecurity incidents classified as level 2 or below should be reported on a monthly basis, at a minimum, to the organization Information Security Official and DHHS PSO in the form of a high-level roll-up.

The DHHS PSO, acting on behalf of the department, will report incidents to the Enterprise Security and Risk Management Office as required by N.C.G.S. §147-33.113 and in accordance with the Statewide Information Security Manual Section on Reporting Information Security Incidents.

The DHHS PSO, acting on behalf of the department, shall determine what, if any, outside authorities need to be contacted in regard to confirmed significant cybersecurity incidents in accordance with applicable regulations and procedures as well as in accordance with federal requirements (e.g. DHHS Department of Public Affairs Office, law enforcement or federal agencies).

10.1.1 Reporting Incidents Involving Social Security Administration (SSA) Data

In the event that an incident involves the disclosure of SSA Data, suspected or confirmed, Divisions and Offices must notify the DHHS PSO by phone within one (1) hour in addition to the online security incident reporting requirements (see the DHHS PSO Website for up-to-date contact information).

10.1.2 Reporting Incidents Involving Federal Tax Information (FTI)

Upon discovering a possible (i.e., suspected or confirmed) improper inspection or disclosure of FTI, including breaches and security incidents, the individual, or their organization, making the observation or receiving information must contact the DHHS PSO by phone within twenty four (24) hours in addition to the online security incident reporting requirements (see the DHHS PSO Website for up-to-date contact information).

10.1.3 Reporting Incidents Involving Centers for Medicare & Medicaid Services (CMS)

In the event an incident occurs that involves the suspected or confirmed disclosure of CMS Data, DHHS Divisions and Offices are required to notify the DHHS PSO by phone within one (1) hour. Additionally, users must follow the standard practice of reporting the incident using the online security incident reporting website (see the DHHS PSO Website for more information).

10.1.4 Incident Categorization and Severity

Incidents are to be classified according to both category and severity level in order to assist in prioritizing responses and baseline impact. In order to reduce complexities in incident reporting, DHHS has broken incidents down into seven general categories:

- **Denial of Service (DoS) -** an attack that prevents or impairs the authorized use and availability of networks, systems, or applications by exhausting resources or forcing software reset
- **Network Probing -** unauthorized network mapping, port probing, security scanning etc. (i.e., checking Department networks to see if there is a possible way in)
- **Malicious Code -** a virus, worm, Trojan horse, or other code-based malicious entity that infects a host
- **Unauthorized Access -** a person gains logical or physical access without permission to a network, system, application, data, or other resource
- **Inappropriate Usage** - a person violates acceptable computing use policies (e.g. an individual with right to access a system looks up/uses information contained within the system for their own personal gain)
- **Criminal -** an incident involving a criminal offence (e.g. theft, fraud, etc.).
- **Multiple Component -** a single incident that encompasses two or more incidents (e.g. a malicious code infection leads to unauthorized access to a host containing departmental data

For incident severity, DHHS mirrors the state's five levels of severity which are designed to subjectively measure incidents based on their potential to negatively impact Department operations, finances or public image. The characteristics in the table on page 61 below are designed to serve as general guidelines only, and are to not be interpreted as absolutes.

-- Remainder of Page Intentionally Left Blank –

Incident Severity	Incident Characteristics
Severe	• Successful penetration or denial-of-service attack(s) detected with significant impact on DHHS operations: ○ Very successful, difficult to control or counteract ○ Large number of systems compromised ○ Significant loss of confidential data Public disclosure of confidential data ○ Loss of mission-critical systems or applications • Significant risk of negative financial or public relations impact • Unresolved critical severity level security vulnerabilities as identified by DHHS Privacy and Security Office • Theft or property damage greater than $10,000.00 • Child Pornography
High	• Penetration or denial-of-service attack(s) detected with limited impact on DHHS operations: ○ Minimally successful, easy to control or counteract ○ Small number of systems compromised ○ Little or no loss of confidential data Individual unauthorized access to confidential data ○ No loss of mission-critical systems or applications • Widespread instances of a new computer virus or worm that cannot be handled by deployed antivirus software • Small risk of negative financial or public relations impact • Unresolved high severity level security vulnerabilities as identified by DHHS Privacy and Security Office • Theft or property damage of $1,000.00 to $10,000.00 • Operation of an illegal download server (i.e., warez server)
Elevated	• Significant level of network probes, scans and similar activities detected indicating a pattern of concentrated reconnaissance • Penetration or denial of service attack(s) attempted with no impact to DHHS operations • Widespread instances of a known computer virus or worm, easily handled by deployed anti-virus software • Isolated instances of a new computer virus or worm that cannot be handled by deployed anti-virus software • Incidents involving intentional or unintentional harassment • Threats to individuals • Unresolved low and medium severity level security vulnerabilities as identified by DHHS Privacy and Security Office • Theft or property damage under $1,000.00

	• Use of Peer-to-Peer (P2P) software for the sharing/download of inappropriate or copyrighted material • Viewing of inappropriate material
Guarded	• Small numbers of system probes, scans, and similar activities detected on external systems • Intelligence received concerning threats to which agency systems may be vulnerable
Low	• Small numbers of system probes, scans, and similar activities detected on internal systems • Isolated instances of known computer viruses or worms, easily handled by deployed anti-virus software

-- End of Document –

CHAPTER 11: NC DHHS Security Manual Updates

Version	Policy Section	Review Mo/Yr	Revision Mo/Yr	New/Revision Language
v01_01	6.5 Vulnerability Management	11/2019	11/2019	1. It is the responsibility of the ISO and/or Privacy Official to monitor and track the remediation process with the business owner of the affected system or application and request the PSO to validate the remediation of any vulnerabilities remaining. 2. If vulnerabilities are not remediated within the required response time, the ISO and/or Privacy Official should escalate to their Division Director and Deputy Secretary and notify the Department Chief Information Officer of the escalation. Where any of the security findings are unable to be remediated, a formal exception will need to be filed. The ISO and/or Privacy Official will need to work with the system owner to request an exception through DHHS.SecurityExceptions@dhhs.nc.gov. Note: Only findings that violate State Standards may have exceptions. Inclusion of any compensating controls, which may act as remediation of risk, will assist in the exception process. Division ISOs and/or Privacy Officials responsible for these tasks can request from the PSO a copy of the DHHS Privacy and Security Office Vulnerability Scanning Methodology and Standard Operating Procedures, which provides additional details regarding ISO and/or Privacy Officials responsibilities in monitoring reported vulnerabilities.
v01_01	Ch. 10 Incident Response	11/2019	11/2019	1. Changes to modify term of security incident to "significant cybersecurity incident" throughout the section in accordance with NC House Bill 217.
v01_02	1.2.4 Maintenance, Reviews and Updates	5/2020	5/2020	1. **New language:** Chapter 1, Section 1.2.4 NC DHHS Security Manual reviews and updates shall be conducted on an annual basis. New policies shall be reviewed by the DHHS Privacy and Security Office and routed to authorized personnel for approvals. Material revisions shall be reviewed and approved at the discretion of authorized personnel. Policies shall be approved prior to publishing to make accessible for all Divisions and Offices. All approved policies shall be provided to Divisions and Offices to include documentation of review dates, update dates, and approval dates for maintenance. NC Divisions and Offices shall maintain their program specific policies and procedures and ensure they align with DHHS Security Manual where applicable to include annual review, updates, and documentation of approval and enforcement. Updates to the Statewide Information Security Manual shall be reviewed annually and as made available by the North Carolina Division of Information Technology. Updates to the Statewide Information Security Manual shall be reviewed annually and adopted within 90 days where there are more restrictive implementation requirements that impact NC DHHS Offices and Divisions. Version control numbers will be assigned based on type of revision as minor or major. Minor revisions will show version control number (vX_XX), major revisions will show v(XX). "v" shall mean version and "XX" indicates the number.
v01_02	1.3 Applicability	5/2020	5/2020	1. **New language:** Division and Office shall develop policy and procedure where there are program specific federal requirements as applicable and are not less restrictive than this policy manual and the Statewide Information Security Manual. Contracts with vendors shall

				reflect the grace period of 90 days to implement applicable change and addendums into the contract language.
v01_02	5.5.4 Dispose of Hardware and Software			1. **New language:** A formal process shall be implemented for the authorization of the removal of equipment from a state operated facility or vendor. Removal shall be requested in writing and authorized. Any exceptions to this requirement shall also be in writing.
v01_02	7.7 Physical Security	5/2020	5/2020	1. **Revision:** In addition to the Statewide Information Security Manual policy (SCIO-SEC-313-00), visitor policies shall include the requirement to ensure visitor records are publicly accessible for a minimum of 2 years.
v01_02	7.8 Access Controls	5/2020	5/2020	1. **New Section: 7.8 Access Controls** In accordance with the NC Statewide Information Security Manual "Access Control" policy, NC DHHS will perform regular access control reporting. Reports will be submitted to the Privacy and Security Office at the end of the month following the quarter.
v01_02	7.8.1 Identification and Authentication	5/2020	5/2020	1. **New Section**: **7.8.1 Identification and Authentication** NC DHHS Division and Offices information systems shall be configured to uniquely identify and authenticate users or processes. Access to NC DHHS information systems shall be through local or network access. At a minimum, this process shall ensure the following; • Prohibition of shared accounts • Information system level and application level mechanisms as determined by a risk assessment; and • Access to all accounts (local, privileged, non-privileged) shall be authenticated using multifactor authentication (MFA). MFA shall be used under the following conditions: o Remote access to information systems using privileged accounts o Remote access to information systems using privileged and non-privileged accounts for information systems that receive, process, store, or transmit federal tax information (FTI), personally identifiable information (PII), protected health information (PHI), or other highly confidential data NC DHHS Division and Offices shall require that all users accessing NC DHHS networks adhere to required security configurations for their devices, including required patches and updated anti-virus signature files. All information systems, including cloud services, shall include the following at a minimum; • Obtain authorization from the security manager • Ensure single users or devices have a single unique identifier that identifies an individual, group, role, or device • Prevent reuse of identifiers for seven (7) years • Disable identifiers after 120 days of inactivity unless exempted by management • Delete or archive identifiers that have been disabled for more than 365 days • Disable accounts within 60 days of inactivity for user and non-user accounts **Guidelines** NC DHHS shall manage information system authentication requirements. Individual authenticators include passwords, tokens, biometrics, PKI certificates, and key cards. NC DHHS shall require the at least the minimum guidelines outlined in the NC DIT Statewide Information Security Manual.

V01_02	7.9 Capital Planning and Budgeting	5/2020	5/2020	1. **New Section: 7.9 Capital Planning and Budgeting** Divisions and Offices authorizing officials typically have budgetary oversight for an information system or are responsible for the business operations supported by the system. The authorizing official shall meet the requirements of the North Carolina Office of Budget and Management's information security budgeting policy through their project request process.
v01_02	4.1 System Development Life Cycle	5/2020	5/2020	1. **Added Language: 4.1 System Development Life Cycle-** To ensure privacy and data protection is incorporated into the SDLC process, Divisions and Office's SDLC shall, at a minimum, include the following data protection steps into the five phases mentioned above: • **Phase I - Requirements:** Perform an initial Privacy Threshold Assessment (PTA), Privacy Impact Analysis (PIA); Review privacy and information security policies, standards, and controls to ensure they are following requirements for collection, use, retention, and disposal of personal data • **Phase II - Design:** Minimize data and perform a formal PTA and PIA; analyze relevant privacy controls to ensure they are designed, developed, and implemented; design and implement feedback control privacy mechanisms into system • **Phase III - Develop:** Obtain initial data subject consent on personal data collection, use, disclosure and retention; ensure transparency where data subjects understand systems and process; ensure data subjects are informed on how to access their personal data and ensure it is up to date and accurate; implement security measures to ensure protection of personal data; perform ongoing testing and evaluation • **Phase IV - Test:** Monitor and report privacy controls through periodic testing and evaluation • **Phase V - Deploy:** Integrate new privacy protection methods or controls into systems for improved privacy; analyze privacy policies, standards and procedures and system performances for irregularities • **Phase VI- Maintenance:** Ensure proper management of new applications and technology in production.
v01_02	7.2.1 Remote Access	5/2/2020	5/2/2020	1. **New Section: 7.2.1 Remote Access** Divisions and Offices must ensure its authorized users of DHHS computer systems, state network, and data repositories are permitted to remotely connect to those systems for the sole purpose of conducting DHHS related business. For purposes of this manual and in accordance with the NC DIT State Information Security Manual, **Remote Access** shall mean the ability of a resource to access the state's network via an external network connection. Remote access generally occurs from remote locations such as homes, hotel rooms, and off-site offices. Remote connections shall be accessed only through a secured, authenticated, and protected access method. At a minimum, the following remote user access guidance shall be implemented: • Authentication and authorization systems for remote access shall be managed by the Divisions and Offices using the North Carolina Identity Management Service (NCID). • Multifactor Authentication (MFA) must be used for remote access to all applications.

				• Revocation/Modification of remote access shall occur at any time for reasons including noncompliance with security policies, request by the user's supervisor, the Division Information Security Official (ISO), or if there is a negative impact on overall network performance attributable to remote connections. • There shall be certain remote access users who warrant use of file and/or disk encryption technology. This shall be based on whether confidential records are included in the information that they are able to store on their local systems. • Audit logs of remote access activities shall be maintained for at least ninety (90) days. **Guidelines** Divisions and Offices shall ensure than remote access to any DHHS resource from an external or non-state source must originate through a virtual private network (VPN). Any other remote access utilities must have specific authorization from the Division Information Security Official (ISO) for their use.
v01_02	5.4.3 Continuous Monitoring	5/2/2020	5/2/2020	1. **New Language:** The State Chief Information Officer (SCIO), shall ensure State agencies and State data are operating in compliance with established enterprise security standards. The Continuous Monitoring Plan shall monitor and ensure that all agencies are assessed using one or a combination of assessment methods: • Third Party Independent Assessment (Vendor or National Guard) • Self-Assessment. The annual assessments and compliance reporting will allow the monitoring of cyberdeficiencies. Any software applications identified as unauthorized or "blacklisted" will be provided by the NCDIT as necessary. The "blacklisted" software applications will be removed from applicable Divisions and Offices.
	1.2.1 Alignment with the Statewide Information Security Manual	4/21/2022	4/21/2022	1. **New Language:** Statewide Information Security Manual is now based off of NIST 800-53 R4
		10/27/2022		Reviewed; no changes made
V01_03	7.8 Access Controls	12/14/2023	12/14/2023	Updated Access control review for Report Period October, November, December to include All Users instead of administrative users
	2.7	12/30/2024	12/30/2024	Updated language regarding AUP and included a link to access the stand alone version of the AUP.
	10.1.3	12/30/2024	12/30/2024	Updated PSO link for reporting incidents involving CMS data
	7.4	12/30/2024	12/30/2024	Removed out of date link to old DIT security policy
	URL validation	12/30/2024	12/30/2024	Reviewed/updated urls to ensure they were valid