

# NC DHHS Security Policy Summary

Security policies can be found online at:

<http://info.dhhs.state.nc.us/olm/manuals/dhs/pol-80/man/index.htm>

A glossary of security terms can be found at: <http://info.dhhs.state.nc.us/olm/manuals/dhs/pol-80/man/Glossary1.htm>

Policy	Division Security Responsibility
<p>Acceptable Use for DHHS Information Systems Policy  <a href="http://info.dhhs.state.nc.us/olm/manuals/dhs/pol-80/man/12acceptable_use1.htm">http://info.dhhs.state.nc.us/olm/manuals/dhs/pol-80/man/12acceptable_use1.htm</a></p>	<p>Each DHHS Division/Office shall be responsible for ensuring that every individual seeking access to DHHS networks and/or information systems reviews this policy and signs an acceptable use agreement based upon the terms specified in this policy.</p> <p>Users must sign the agreement form included before permission granted to use the DHHS systems.</p>
<p>Application Security Policy  <a href="http://info.dhhs.state.nc.us/olm/manuals/dhs/pol-80/man/15application_security1.htm">http://info.dhhs.state.nc.us/olm/manuals/dhs/pol-80/man/15application_security1.htm</a></p>	<p>DHHS Divisions/Offices shall implement application security standards to have effective controls over systems they directly manage. These security controls will vary in accordance with the sensitivity and criticality of each application. This policy addresses the following requirements: (1) application security standards and implementation guidelines; (2) the implementation of security controls during the system's lifecycle; and (3) security documentation.</p>
<p>Business Continuity &amp; Disaster Recovery Plan(s) Policy  <a href="http://info.dhhs.state.nc.us/olm/manuals/dhs/pol-80/man/Business_Continuity_and_Disaster_Recovery_Plan_1.htm">http://info.dhhs.state.nc.us/olm/manuals/dhs/pol-80/man/Business_Continuity_and_Disaster_Recovery_Plan_1.htm</a></p>	<p>All DHHS Divisions and Offices shall develop, review and update information technology business continuity plans (BCP) and disaster recovery (DR) plans as part of an IT Business Continuity Management Program to ensure the timely and reliable access to critical automated business services.</p>
<p>Business Impact Analysis Policy  <a href="http://info.dhhs.state.nc.us/olm/manuals/dhs/pol-80/man/09business_impact_analysis1.htm">http://info.dhhs.state.nc.us/olm/manuals/dhs/pol-80/man/09business_impact_analysis1.htm</a></p>	<p>The DHHS Division/Office Directors, managers and business owners are responsible for determining the criticality of their operations. Each DHHS Division/Office is responsible for ensuring that contingency plans have been implemented. The BIA is used to accomplish this objective and is used to analyze the service workflow, which typically consists of both manual and automated (IT Services) components.</p>
<p>Security for Information System Contracts Policy  <a href="http://info.dhhs.state.nc.us/olm/manuals/dhs/pol-80/man/04contract_security1.htm">http://info.dhhs.state.nc.us/olm/manuals/dhs/pol-80/man/04contract_security1.htm</a></p>	<p>DHHS Divisions/Offices shall be responsible for providing contract management and oversight on IT contracts. Contract management may be provided either directly or contracted to the Division of Information Resources Management (DIRM). Divisions/Offices may add additional language to contracts in order to meet division-specific funding requirements or implement division-specific procedures or reporting requirements.</p>
<p>Data Classification, Labeling and Access Control Policy  <a href="http://info.dhhs.state.nc.us/olm/manuals/dhs/pol-80/man/10data_classification1.htm">http://info.dhhs.state.nc.us/olm/manuals/dhs/pol-80/man/10data_classification1.htm</a></p>	<p>DHHS Divisions/Offices shall be responsible for implementing data classification, labeling, and control procedures. The classification and assignment of security levels will be maintained by DIRM. Divisions/Offices shall also be responsible for reviewing and updating the inventory and submitting updates of information in a timely manner.</p>

## NC DHHS Security Policy Summary (cont)

Policy	Division Security Responsibility
<p>Data Protection Policy  <a href="http://info.dhhs.state.nc.us/olm/manuals/dhs/pol-80/man/11data_protection1.htm">http://info.dhhs.state.nc.us/olm/manuals/dhs/pol-80/man/11data_protection1.htm</a></p>	<p>The DHHS Privacy &amp; Security Office (PSO) shall develop data protections standards and implementation guidelines for all applications. In this context, the DHHS Divisions/Offices shall be responsible for the classification of all data (see Data Classification Policy for details) and for evaluating and ensuring the adequacy of all security controls for applications maintained by the DHHS Divisions/Offices. DHHS data shall be protected from unauthorized or accidental disclosure, misuse, modification or loss.</p> <p>For those applications/systems maintained by DIRM as an affiliate of a Division/Office, DIRM itself shall be responsible for ensuring the adequacy of the security controls.</p>
<p>Information Incident Management Policy  <a href="http://info.dhhs.state.nc.us/olm/manuals/dhs/pol-80/man/19incident_management1.htm">http://info.dhhs.state.nc.us/olm/manuals/dhs/pol-80/man/19incident_management1.htm</a></p>	<p>DHHS Divisions/Offices shall be responsible for managing and reporting all security incidents. The division/office shall rapidly identify, report, manage, mitigate and resolve information security incidents.</p>
<p>Information Security Management Policy  <a href="http://info.dhhs.state.nc.us/olm/manuals/dhs/pol-80/man/02info_security_management1.htm">http://info.dhhs.state.nc.us/olm/manuals/dhs/pol-80/man/02info_security_management1.htm</a></p>	<p>This policy defines the security management requirements for the DHHS Privacy and Security Office (PSO) and the DHHS Divisions/Offices.</p> <p>DHHS Divisions/Offices shall:</p> <ul style="list-style-type: none"> <li>– Create and maintain information security plans.</li> <li>– Define strategies and mitigate risks to acceptable levels for the division.</li> <li>– Determine the sensitivity and criticality of all data used.</li> <li>– Develop, maintain and implement specific security policies, procedures and guidelines to supplement those of the PSO, as required, to meet requirements.</li> <li>– Develop and maintain emergency response, communication, and recovery procedures.</li> <li>– Develop information security control baselines for network, application or information systems in order to objectively evaluate Division/Office security.</li> <li>– Ensure that all staff receives the security awareness training for their workforce provided by the PSO.</li> <li>– Ensure that information resources are properly managed.</li> <li>– Ensure that information security standards are not compromised throughout the change management process.</li> <li>– Ensure that noncompliance issues and other variances are resolved in a timely manner.</li> <li>– Ensure that risk assessments are performed periodically to evaluate effectiveness of existing controls.</li> <li>– Ensure that risk identification, analysis and mitigation activities are performed.</li> <li>– Ensure that services provided by third parties, including outsourced providers, are consistent with established information security policies.</li> </ul>

## NC DHHS Security Policy Summary (cont)

Policy	Division Security Responsibility
	<ul style="list-style-type: none"> <li>- Ensure that the organizational, administrative, physical, and technical procedures for information systems comply with DHHS information security policies.</li> <li>- Establish a business/IT recovery team.</li> <li>- Establish, maintain and implement procedures for documenting incidents as a basis for subsequent investigation.</li> <li>- Evaluate the execution of response and recovery plans and provide feedback for improvement.</li> <li>- Follow documentation review processes/procedures as defined by the PSO.</li> <li>- Implement a change management system with document version control.</li> <li>- Implement a systematic, analytical, and continuous risk management program for information systems.</li> <li>- Implement Data Classification and Control procedures in the work environment.</li> <li>- Implement the Incident Management and Reporting capability.</li> <li>- Implement physical security policies and develop, maintain and implement procedures.</li> <li>- Implement the risk management program for information systems developed by the PSO.</li> <li>- Manage outsourced IT contracts (via a service-level agreement).</li> <li>- Manage post-incident reviews (“lessons learned”) and document incident causes and recommended corrective actions, in consultation with the PSO.</li> <li>- Plan for Business Continuity and Disaster Recovery under the leadership of and following the guidelines and procedures of the PSO.</li> <li>- Promote data stewardship and individual accountability among business process owners, data owners, managers and other stakeholders to manage information security risks.</li> <li>- Provide oversight over IT contracts to ensure compliance with IT security policies.</li> <li>- Provide periodic testing of the response and recovery plans where appropriate, with assistance from the PSO, as necessary.</li> <li>- Report significant changes in risk levels including threats and vulnerabilities to appropriate levels of management on both a periodic and an event-driven basis.</li> <li>- Use the metrics defined by the PSO to measure, monitor and report on the effectiveness of information security controls and compliance with DHHS information security policies.</li> </ul>

## NC DHHS Security Policy Summary (cont)

Policy	Division Security Responsibility
<p>Information Systems Review &amp; Auditing Policy  <a href="http://info.dhhs.state.nc.us/olm/manuals/dhs/pol-80/man/20info_systems_auditing1.htm">http://info.dhhs.state.nc.us/olm/manuals/dhs/pol-80/man/20info_systems_auditing1.htm</a></p>	<ul style="list-style-type: none"> <li>- All DHHS critical applications and systems shall be audited/reviewed after being placed into production. The audit frequency shall be on a periodic basis. Assessment and operational reviews shall be conducted based upon the criticality and risk level of the application.</li> <li>- An IS review or audit process shall be implemented to evaluate information systems.</li> <li>- DHHS Divisions/Offices should conduct periodic security self-assessments.</li> <li>- If a DHHS Division or Office has outsourced work to a contractor, they are responsible for providing oversight to ensure the contractor is providing adequate security.</li> </ul>
<p>IT Inventory Management &amp; Control Policy  <a href="http://info.dhhs.state.nc.us/olm/manuals/dhs/pol-80/man/08IT_inventory_manage_control1.htm">http://info.dhhs.state.nc.us/olm/manuals/dhs/pol-80/man/08IT_inventory_manage_control1.htm</a></p>	<p>The DHHS Division of Information Resource Management (DIRM), shall establish, manage and maintain an inventory of all IT resources for the department. DIRM shall accomplish this by working directly with the DHHS Divisions/Offices. These procedures shall also include monitoring and the updating of the inventory as well as validating the information collected.</p> <p>DHHS Divisions/Offices shall be responsible for implementing data classification, labeling, and control procedures. They shall also be responsible for reviewing and updating the inventory and for submitting updated information in a timely manner.</p>
<p>IT Operations Security Policy  <a href="http://info.dhhs.state.nc.us/olm/manuals/dhs/pol-80/man/14IT_operations_security1.htm">http://info.dhhs.state.nc.us/olm/manuals/dhs/pol-80/man/14IT_operations_security1.htm</a></p>	<p>If a DHHS Division/Office maintains its own applications and systems, its staff shall be responsible for implementing the security of those operations through adherence of the DHHS Privacy and Security Office policies and standards.</p> <p>If the DHHS Divisions/Offices have IT operations that are being handled by a contractor/vendor, the Division or Office shall provide contract management oversight to ensure that adequate security is being provided. New and renegotiated contracts shall outline the security requirements to be met.</p>
<p>Personnel Security Policy  <a href="http://info.dhhs.state.nc.us/olm/manuals/dhs/pol-80/man/05personnel_security1.htm">http://info.dhhs.state.nc.us/olm/manuals/dhs/pol-80/man/05personnel_security1.htm</a></p>	<p>DHHS Division/Offices will map personnel position with the classification levels and monitor all changes to the job positions. Likewise, all DHHS contracts shall be reviewed to ensure the proper classification levels have been met.</p>

## NC DHHS Security Policy Summary (cont)

Policy	Division Security Responsibility
<p>Physical &amp; Environmental Security Policy  <a href="http://info.dhhs.state.nc.us/olm/manuals/dhs/pol-80/man/07physical_env_security1.htm">http://info.dhhs.state.nc.us/olm/manuals/dhs/pol-80/man/07physical_env_security1.htm</a></p>	<ul style="list-style-type: none"> <li>– All DHHS Division/Office Managers and Supervisors responsible for operations shall ensure that adequate physical security is provided to protect assets.</li> <li>– All DHHS Divisions/Offices shall have Facility Management. This function may be outsourced (e.g., with leased buildings) or there may be a DHHS representative assigned to one or more buildings.</li> <li>– All DHHS buildings shall have visitor control procedures.</li> <li>– All DHHS network and computer operations managers/administrators shall be responsible for the physical security of the hardware and software assets assigned to them. The responsibility may lie with DIRM or DHHS.</li> <li>– Contracts administration shall ensure that third party agreements provide the level of security defined in DHHS policies. DHHS contracts and interagency agreements shall contain the necessary physical security provisions to protect sensitive and critical information in the work stream.</li> <li>– Each DHHS facility shall have designated emergency evacuation personnel (Safety Officers) who will ensure that emergency evacuation routes are clearly posted, emergency response procedures are documented, tested and distributed to all building personnel.</li> </ul>
<p>Risk Management Policy  <a href="http://info.dhhs.state.nc.us/olm/manuals/dhs/pol-80/man/03risk_management1.htm">http://info.dhhs.state.nc.us/olm/manuals/dhs/pol-80/man/03risk_management1.htm</a></p>	<p>DHHS Divisions/Offices shall implement the enterprise-wide risk management program developed by the DHHS Privacy and Security Office.</p>

## NC DHHS Security Policy Summary (cont)

Policy	Division Security Responsibility
<p>DHHS Security Organization Policy  <a href="http://info.dhhs.state.nc.us/olm/manuals/dhs/pol-80/man/01security_organization1.htm">http://info.dhhs.state.nc.us/olm/manuals/dhs/pol-80/man/01security_organization1.htm</a></p>	<ul style="list-style-type: none"> <li>- Assign a Division/Office representative to the SWG. This representative shall attend SWG meetings and review the security policies, standards, procedures and guidelines developed and adopted by the DHHS PSO.</li> <li>- Designate a Division/Office Information Security Official or provide contractual oversight in order to implement the Division/Office security program.</li> <li>- Ensure that Division/Office staff and workforce participate in enterprise- wide training provided by the DHHS Privacy and Security Office and supplement the enterprise-wide training with division/office-specific training as needed.</li> <li>- Ensure that the physical security is appropriate at the DHHS Division or Office.</li> <li>- Facilitate or develop, maintain and implement plans, policies, and procedures to ensure the security of information technology within the Division/Office.</li> <li>- Implement a risk management program within the DHHS Division/Office following specific guidelines and procedures created by the DHHS PSO.</li> <li>- Implement Division or Office security requirements by incorporating new security technology and practices into existing information technology environments and business operations, respectively.</li> <li>- Partner with the DHHS Privacy and Security Office to ensure the information security of the Division or Office.</li> </ul>
<p>Security Testing Policy  <a href="http://info.dhhs.state.nc.us/olm/manuals/dhs/pol-80/man/18security_testing1.htm">http://info.dhhs.state.nc.us/olm/manuals/dhs/pol-80/man/18security_testing1.htm</a></p>	<ul style="list-style-type: none"> <li>- DHHS Divisions/Offices shall be notified of any vulnerabilities found during testing and shall review and implement controls to minimize the risk associated with these vulnerabilities.</li> <li>- The Division of Information Resources Management (DIRM) working with the DHHS Privacy and Security Office shall ensure that security testing is performed on all DHHS systems/applications, the network, and the DHHS Physical Infrastructure.</li> </ul>

## NC DHHS Security Policy Summary (cont)

Policy	Division Security Responsibility
<p>Security Training &amp; Awareness Policy  <a href="http://info.dhhs.state.nc.us/olm/manuals/dhs/pol-80/man/06security_training_and_awareness1.htm">http://info.dhhs.state.nc.us/olm/manuals/dhs/pol-80/man/06security_training_and_awareness1.htm</a></p>	<ul style="list-style-type: none"> <li>- Develop and implement non-enterprise level, system-specific training to supplement general security training, in consultation with and assisted by the PS.O</li> <li>- Develop and maintain the summary of enterprise-wide policy, standards, and procedures for distribution to DHHS workforce.</li> <li>- Distribute the summary of enterprise wide policies, procedures and standards, as well as division/office-specific policies, procedures and standards to the workforce.</li> <li>- Ensure that security awareness and training is provided throughout the organization.</li> <li>- Ensure that security awareness presentations are developed to meet Division/ Office specific requirements.</li> <li>- Facilitate the completion of the initial assessment of Division/Office workforce members' security training needs.</li> <li>- Periodically evaluate information security training needs.</li> </ul>
<p>User Authorization, Identification &amp; Authentication Policy  <a href="http://info.dhhs.state.nc.us/olm/manuals/dhs/pol-80/man/13user_authorization1.htm">http://info.dhhs.state.nc.us/olm/manuals/dhs/pol-80/man/13user_authorization1.htm</a></p>	<ul style="list-style-type: none"> <li>- Managers/supervisors - DHHS managers/supervisors have the responsibility of requesting access to information systems and approving user access privileges based upon their assigned duties and notifying the system administrator of changes in access status.</li> <li>- System Administrators - System Administrators have the responsibility of periodically reviewing user access privileges and notifying management of any access concerns. This responsibility may lie with the Division of Information Resource Management (DIRM), an outsourced contractor or within the DHHS Division/Office but shall be in compliance with standards established by the DHHS Privacy and Security Office.</li> <li>- System Owners - System Owners for each information system shall be responsible for ensuring that authorization and account management processes exist for their specific division/office and that the appropriate people have been assigned the responsibility of creating and maintaining the authorization records. The design and development of the authorization and account management processes shall comply with DHHS standards.</li> <li>- DHHS Division/Office System Owners may monitor and/or review the security and privacy policies and operations of an agency, contractor/vendor or individuals as a condition for granting access or as a condition for continued access to information resources.</li> </ul>
<p>Waivers and Appeals Policy  <a href="http://info.dhhs.state.nc.us/olm/manuals/dhs/pol-91/man/Waiver_Appeal1.htm">http://info.dhhs.state.nc.us/olm/manuals/dhs/pol-91/man/Waiver_Appeal1.htm</a></p>	<p>DHHS Divisions/Offices shall follow the DIRM process for requesting and granting waivers to all DHHS information technology policies, standards and requirements. Division/Office directors shall submit written requests to the DIRM director to waive adherence to DHHS ITS policies, standards and requirements. If the request is outside the</p>

## NC DHHS Security Policy Summary (cont)

Policy	Division Security Responsibility
	scope of authority of DIRM, then DIRM shall notify ITS of the request and serve as the point of contact with ITS.
Wireless Security Policy <a href="http://info.dhhs.state.nc.us/olm/manuals/dhs/pol-80/man/21wireless_security1.htm">http://info.dhhs.state.nc.us/olm/manuals/dhs/pol-80/man/21wireless_security1.htm</a>	DHHS Divisions/Offices shall implement security controls that will protect the DHHS wireless infrastructure as well as protect wireless communications: DHHS Divisions/Offices connecting to DHHS networks using wireless systems must meet the criteria of this policy or have a waiver from the DHHS Security Officer.

\*\*\*End of Document\*\*\*