

March 12, 2014 - CLARIFICATIONS AND AMENDMENTS:

CLARIFICATION:

Section 5.3.1, Table 5.3.1-1 – Topics Requiring Narratives, Page 24 of 72 – The topic titles that appear on Table 5.3.1-1 on page 24 do not correlate with the Topic titles on pages 25 through 31. Please do not associate the titles in the table to the topic titles that appear next to each topic on pages 25 through 31.

We have already clarified that Topics 1 through 10 are a maximum of two pages and Topic 11 is unlimited.

CLARIFICATION:

Responses are required for all Topics appearing on pages 25 through 31. Separately, responses are required for all topics on Page 24.

CLARIFICATION:

For those vendors who wish to review the State of New Hampshire's IT Policy & Standards, they are available below:

Reference to RSA, Laws and Regulations may be found at:

<http://www.gencourt.state.nh.us/rsa/>

<http://www.gencourt.state.nh.us/rsa/html/i/21-r/21-r-4.htm>

<http://www.gencourt.state.nh.us/rsa/html/i/21-r/21-r-mrg.htm>

Current DoIT Standards:

WIRELESS GUEST ACCESS POLICY

Purpose: To establish uniform and secure guest access by state and non-state staff utilizing state wireless resources managed by the Department of Information Technology (DoIT).

Policy: Guest wireless access will be provided only to guest users approved by an authorized State agency designee. All guest users must abide by the following conditions of use:

- The State assumes no responsibility for the safety of equipment or device configurations, security, or data files resulting from connection to State guest access.
- All accounts using the Guest wireless network must be created based on least privilege and shortest duration. Start and end dates must be based on need with a system maximum enforced duration in days based on account type.
- Each agency is responsible for the creation of the following accounts using a provided self-service portal:

Account Type	Login Convention: Created by	Maximum Enforced Duration	Personal Device User Agreement Required
Generic Guest	Generic; Sponsor	1 Day	No
Guest: Short-term	Named: Sponsor	10 Days	No
Guest: Long-term	Named: Sponsor	6 Months	Yes
Employee (BYOD)	Named: Sponsor	1 Year	Yes

- Guest User Accounts must be created using the provided Sponsor Portal. The Guest authentication policy configured must meet the Sponsor Portal accounts for authentication.
- Each agency will be provided a Sponsor Portal view that allows them to manage the accounts created by that agency.
- Accounts can be created up to ten (10) days in advance.
- All users of the Guest wireless network must:
 - Utilize their account only for the purposes of connection to the Internet.
 - Accept the usage agreement presented upon login and prior to connection.
 - Be responsible for device setup and troubleshooting; no technical assistance will be provided by DoIT.
 - Be responsible to protect devices through anti-virus, personal firewalls, etc.
 - Notify the Agency when guest access is no longer required.
- Guest access is provided with no guarantee of service as the guest wireless network may be subject to periodic maintenance and unforeseen interruptions.
- The State reserves the right to log usage, filter and/or block access to sites for security reasons.
- Network printing access is not available via guest wireless networks.
- Any attempt to circumvent State procedures or access unauthorized resources, will result in the permanent disconnection from the guest wireless network.
- No state-owned devices are permitted to access any guest wireless solution except in cases where staff wireless is unavailable at a state location. In this case, access to State resources must be done via the State-provided secure VPN.

Accountability: All authorized guest users of any state and/or agency wireless network shall adhere to this policy. It is the responsibility of all agency heads or their designee to enforce this policy. Employees who do not comply with this policy shall be subject to disciplinary action as outlined in the Administrative Rules of the Division of Personnel.

DATA CLASSIFICATION POLICY

Purpose: The purpose of this policy is to establish a uniform method of data classification to safeguard data and promote compliance with state and federal laws and regulations including, but not limited, RSA Chapter 91:A, New Hampshire's Right to Know law regarding the privacy and confidentiality of publicly owned information. Although this policy is applicable to all state computing systems managed by the Department of Information Technology (DoIT), it is relevant to both digital and non-digital state data.

Policy: The classification of data determines the extent to which data should be secured to protect the confidentiality, integrity and availability of information. Data classification differentiates between data which is openly disclosable to the public and that which is highly confidential or private in nature.

Classification. Each state organization is considered the data owner of information within their agency. Although DoIT maintains an agency's digital information, the data owner is responsible for classifying data under their control into the following classifications:

Classification	Description	Examples
Public	Information available to the general public with no restrictions on access or usage	Agency locations and hours; contact information; press releases; pamphlets; public access web sites
Non-Public	Information not disclosable to the public. Can be designated into the following categories:	Data protected by RSA Chapter 91:A
Internal	Information critical to on-going operations which should not be copied, shared, or removed outside of the organization without authority. Also known as "For Official Use Only" (FOUO) data.	Configuration standards; disaster recovery plans; procedures; employment and training program data
Restricted	Information for use by authorized personnel only and not for circulation. Information protected by federal or state regulations. Also known as "Confidential" data.	Medical records, network diagrams, data protected by law such as HIPAA; Personally Identifiable Information (PII); Federal Tax Information (FTI); criminal history data

NOTE: Data classification within the Non-Public classification refers to the most sensitive component; when combining datasets of differing subcategories, the category assigned must be equivalent to the most sensitive or restrictive category of any dataset.

Handling. The storage and handling of information is governed by the classification and Non-Public categorization.

Classification	Storage/Handling	Transmission	Destruction
Public	No restrictions	No restrictions	No restrictions
Non-Public	Restricted access; recommend directory structure to match categorization	See categories below	See categories below

END-USER ACCOUNT AND PASSWORD POLICY

Purpose: The purpose of this policy is to establish uniform standards for the implementation and management of end-user accounts used by the general public or agency constituents to access state applications. This policy does not apply to applications that use Active Directory for authentication and authorization.

Policy: The user login shall consist of a minimum of eight (8) alpha-numeric characters. User names must be unique; shared user names are not permitted.

A password change will be required at initial login and subsequently on an annual basis.

The table below defines the password criteria and policy:

Minimum password length	Eight (8) characters
Password Format	<p>Passwords must contain at least one:</p> <ul style="list-style-type: none"> • Uppercase character • Lowercase character • Number <p>Password may contain non-alphabetic characters such as @, &, %, !</p> <p>When non-alphabetic characters are permitted, user instructions must clearly identify which characters are allowed.</p> <p>It is recommended, but not mandatory, that passwords not contain</p> <ul style="list-style-type: none"> • Any part of the user name • Dictionary words • Keyboard sequences
Maximum password age	An age to be set within the application, not to exceed 360 days
Minimum password age	An age to be set within the application, not to be less than zero (0) days
Enforce password history	A history to be set within the application, not to be less than one (1)
Account Lockout Threshold	A threshold to be set within the application, not to be more than five (5)
Reset Account Lockout Counter After	A reset counter to be set within the application, not to be less than five (5) invalid attempts
Account Lockout Duration	A lockout duration to be set within the application, not to be less than five (5) minutes

Note: In the event the application uses Active Directory for authentication and authorization, then all user accounts and passwords shall comply with the statewide User Account and Password Policy.

ENTERPRISE SECURITY POLICY

Purpose: The purpose of this document is to define the statewide security policy to protect the State network resources and information systems managed by the Department of Information Technology (DoIT).

Policy: Statewide and DoIT policies, procedures and configuration standards defining technical, management and operational controls are in place to ensure the confidentiality, integrity, and availability of state information resources. All devices and products procured must meet current standards and be deployed in compliance with standards.

The following details key security components and requirements:

Network Security. Network devices including firewalls, intrusion prevention systems (IPS), routers, switches, wireless, and remote access solutions (IPSec and SSL VPN) must be configured to meet appropriate configuration standards. Devices must be maintained with current operating systems and signatures, and where possible, be configured to block potentially malicious and/or unauthorized traffic. Devices must be configured to feed into the core Security Information and Event Management (SIEM) platform to allow traffic aggregation and correlation in order to detect unusual and/or unauthorized activities.

Internet Security. Internet browsing is a primary mechanism for the introduction of malicious code such as malware and viruses. An internet security platform must be implemented and maintained to reduce this exposure. Access to high risk security site categories must be blocked except by approved exception. Site access will be based on agency-defined business requirements and as approved by an agency authorizer via the posted Internet access request procedure. Client-based safety rating tools implemented must be configured to block access to high rated, known malicious sites. Access to additional sites may also be blocked at the state edge based on security advisories.

Email Security. Email security must be implemented at the internet edge and/or email servers on all inbound and outbound email traffic. Inbound coverage must automatically reject email from untrusted sources, containing viruses or identified as malicious spam. Questionable email will be identified and quarantined for user review, deletion or release. The email security gateway must use an anti-virus product which varies from the client-based solution.

Host Security. Servers must be configured to meet configuration and policy standards; be maintained at the most current operating system and application level possible with relevant patches, service packs and hot fixes; have services limited to only those required; have administrative and user access accounts based on least privilege; and have required logging enabled. The statewide vulnerability management system must be used to identify potential vulnerabilities and verify remediation on a routine basis. On application servers, file integrity monitoring must be utilized where required and funded for regulatory compliance.

Application Security. Systems must meet all application security requirements. Security must be addressed throughout the entire application life cycle from planning to deployment into production as defined in the Agency Software Division (ASD) System Development Methodology (SDM). Coding must meet standards to reduce exposure such as cross-site scripting, and include syntax validation of inputs.

Client Security. Client devices including desktops, laptops, and other mobile and/or peripheral devices must be configured according to configuration and policy standards and be centrally maintained with updated anti-virus and anti-malware software to reduce

EXTERNAL LINKING POLICIES

Purpose: State agency websites shall establish and enforce explicit agency-wide linking policies describing management controls for linking to external websites. These policies shall include not just basic linking to external sites but also encompass any marketing or advertisement links.

Policy: To establish and enforce agency wide external linking policies.

The State of New Hampshire does not intend to support external websites that are open public forums. For that reason links to external content on State of New Hampshire websites shall meet clear business objectives of the agency and shall appropriately limit linking to information and services to that which is necessary for the proper performance of agency functions.

Description: Agencies shall establish external linking policies that appropriately limit external linking to information and services to that which is necessary for the proper performance of an agency function. The policy must include reasonable management controls to assure the external links remain active or otherwise continue to provide the level of quality (including objectivity, utility and integrity) as intended by the agency and expected by visitors. Therefore, when an agency determines external links are necessary, they must take reasonable steps to ensure the presentation is accurate, relevant, timely and complete.

Agency links to commercial organizations and special interest groups present special challenges with respect to maintaining agency objectivity and avoiding the appearance of endorsement of particular products or viewpoints and thus must be used judiciously.

Agencies may include acknowledgements to partners or program sponsors on their websites as long as the acknowledgement is made discretely and it is accompanied by a disclaimer that the acknowledgement does not constitute an endorsement.

Agencies that include a web directory with links to external websites must define the class of entities that may be listed in the directory, permit anyone within that class to be linked and disclose the criteria and procedures for requesting a link. Agencies should consult with the Attorney General's Office before establishing any class of permitted entities that would allow links to sites making political speech or which endorse or oppose particular public policies. Web directories shall include a disclaimer that inclusion in the directory does not constitute an endorsement.

When an agency website requires the use of particular software that a visitor may need to download (e.g. Adobe Acrobat Reader required for PDF files), the link to the download site may be included. The link shall be accompanied by a statement that the particular software is required.

Accountability: This policy pertains to all State of New Hampshire agency websites and applications and to their administrators. State agencies shall designate a staff member to be responsible for incorporation of this Policy. This responsibility includes the dissemination of any additional guidelines, standards and compliance monitoring reports to the appropriate staff. Appropriate staff includes, but is not limited to, agency employees responsible for site administration or content development as well as any consultant or vendor responsible for an agency website and/or content.

It is the responsibility of each Agency/Department/Division/Bureau Chief or their designee to enforce this policy.

Reference: IT Standards Exception Policy

Page 1 of 1

Department of Information Technology – Office of the Chief Information Officer (CIO)

Effective – 11.05.2007

HOSTED SOLUTIONS POLICY

Purpose: The purpose of this policy is to ensure functional and secure solutions for external cloud-based services and/or hosted solutions contracted by State agencies and reviewed through the Department of Information Technology (DoIT).

Policy: All external cloud-based services and hosted solutions must meet operational and security requirements to protect the confidentiality, integrity and availability of State information. These solutions are determined viable when there is a defined business justification, identification and acceptance of risk, and a determination of cost effectiveness.

The National Institute of Standards and Technology (NIST) defines cloud computing as ‘a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction.’ Cloud computing is typically determined feasible in instances where computing services can be used to improve the efficiency of organizations with minimal risk and at reduced cost.

Hosted solutions are when a contracted entity procures the hardware and software necessary to meet a business need, and is responsible for all day-to-day management. Hosted solutions are typically used to reduce startup costs associated with a solution and IT resources required to maintain a solution.

The following checklist must be included and addressed in all contracts for external cloud computing services and/or hosted solutions:

Item	Contract Requirements
Availability	<ul style="list-style-type: none"> • Availability percentage must exceed 99.9% • Must specify how percentage is calculated • Must specify compensation if availability fails
Data Preservation	If the contract is terminated either by the vendor or the State, the vendor must be obligated to preserve data and provide it to the State in an agreed upon format within 90 days.
Physical	<ul style="list-style-type: none"> • Dedicated data center facility at specified location • Facility with redundant, tested disaster recovery site • Video surveillance of facility and perimeter • Humidity and temperature control • Raised floor • UPS and generator system with on-site fuel storage of a minimum of 36 hours for the generator • Fire detection and suppression systems • Equipment and systems in access-controlled areas • Facility designed to withstand environmental damage such as from fire, floods, and hurricanes. • Asset management system in place
Personnel	<ul style="list-style-type: none"> • Background checks required • Physical and electronic access based on least privilege • Signed computer use agreement, refreshed annually • Cybersecurity awareness training, refreshed annually

INFORMATION RISK MANAGEMENT POLICY

Purpose: The purpose of this document is to define a uniform and effective information risk management policy for State systems and information.

Policy: Information risk management plays a critical role in protecting State's information assets by allowing risk informed decisions at the organization, business process, and information system levels. An ongoing, holistic effort is required to identify, analyze, and take mitigative steps to reduce risk to an acceptable level in people, process, and technology components of State information systems.

Risk management should be routinely conducted by each agency based on information system classification in consideration of confidentiality, integrity, and availability factors. Risk assessment, a key component of risk management, should be conducted bi-annually on all State systems containing confidential data or at a frequency dictated by regulatory requirements. For example, Payment Card Industry (PCI) environments require an annual risk assessment.

Assessments should be led by the agency Information Security Officer (ISO) or designee and have participation by appropriate system leaders and key stakeholders. Findings should be discussed with agency management, and recommendations presented to, and approved by, the agency Commissioner prior to implementation.

Comprehensive risk management requires collaboration between State agencies as the data owners and input from the Department of Information Technology (DoIT) as the technology resource custodians. Ongoing bi-directional information and communications flows are required for risk management activities to work efficiently and effectively.

The referenced information classification matrix, risk assessment template and all other supporting information, such as system documentation and survey responses, should be retained at the agency by the ISO or designee.

Accountability: It is the responsibility of each Agency Head or designee to enforce this policy. Employees who do not comply with this policy shall be subject to disciplinary action as outlined in the Administrative Rules of the Division of Personnel.

Description: Information risk management plays a critical role in protecting State's information assets. This policy has been reviewed and approved by the Cybersecurity Advisory Council.

Reference: Information Risk Assessment Procedure
Information Classification Matrix Template
Risk Assessment Template
System Management Survey

IT STANDARDS EXCEPTION POLICY

Purpose: The purpose of this policy is to acknowledge that in certain specific instances a situation may exist where an agency, based on the unique characteristics of its mission and financial situation, could be unduly burdened by the enforcement of specific IT standards, policies and procedures. In these cases, an exception to this policy can be requested.

Policy: Exceptions to IT policies and procedures are only granted when the agency demonstrates that enforcement of a specific policy creates a substantial burden on the agency. The exception must not create an undue risk to the agency, the State or the State's IT infrastructure.

Exception Requests:

The Agency Head or designee of an agency seeking an exception must make a written request to the Department of Information Technology (DoIT) Chief Information Officer (CIO) or send an email request to CIOApproval@doit.nh.gov that:

1. Clearly defines the policy or procedure to which an exception is sought.
2. Specifies who and/or what devices an exception is being requested.
3. Demonstrates that enforcement would create a substantial burden on the agency.
4. Demonstrates that the exception will not create undue risk to the agency or the State.
5. Contains an affirmative statement that the Agency Head considers the benefit of the exception to outweigh any risks created by the exception and is willing to accept the additional risk.

Approved exceptions no longer required due to a change in business and/or employee requirements must be reported to DoIT-Security@doit.nh.gov so the exception can be updated and closed.

Accountability: All authorized users of any state and/or agency network must adhere to this policy.

It is the responsibility of all Agency Heads or designee to enforce this policy. Employees who do not comply with this policy shall be subject to disciplinary action as outlined in the Administrative Rules of the Division of Personnel.

Any exceptions granted shall be reviewed by the DoIT IT Security Group (ITSG) as necessary based on the nature of the exception to determine if the current circumstances warrant the continuation of the exception.

Description: This policy serves to protect state networks at the same time give the agency the avenue to request exception.

MOBILE DEVICE SECURITY POLICY

Purpose: The purpose of this policy is to establish safeguards for the use of state-owned mobile computing and portable media storage devices serving to protect state data, networks, and applications.

Policy: Mobile computing devices include laptops, hand held computers, personal digital assistants (PDAs), smart phones and portable media storage devices including, but not limited to, flash memory (memory sticks), flash cards, portable hard drives, and MP3 players.

Mobile technologies are expanding in capability while declining in cost, increasing their popularity and use by varying types of mobile workers. Although these devices offer mobility conveniences and provide productivity benefits outside of the workplace, they introduce a security risk. Given their small size and portability, key security concerns include exposure of critical information, loss or theft of devices, and virus propagation. This policy will define the physical and data security measures established to mitigate the risk of exposure and/or loss of business and confidential state agency data.

Mobile devices will only be provided when business justification and agency head approval is provided. An inventory of all mobile devices must be maintained with documentation by the responsible agency on a routine basis. The theft or loss of mobile devices must be reported immediately. Mobile devices are subject to periodic policy compliance audits by the Department of Information Technology (DoIT.) The use of personal mobile devices is prohibited.

Controlled physical access is the best defense to protect data stored on mobile computing devices. Users assigned mobile devices must abide by the following physical security requirements:

1. Device must be used only by the assigned employee; devices are not to be given to or used by any other state employee or other person.
2. Device must contain only data limited to what is required and authorized.
3. When not in use, devices must be stored in a secure environment to minimize the risk of theft or unauthorized use.
4. Device must not be left unattended in insecure areas where unauthorized access is possible.
5. Care should be taken when using devices in public areas where unauthorized viewing is possible.
6. Device must be "Shut Down" when not in use. Device must not be left in hibernate, suspend or sleep mode and should only be left in password locked/screen saver mode when in a secured area.
7. Internal and external access to state network resources requires the use of a secure VPN connection or other approved access solution.

All mobile devices will be configured/maintained with the following for safeguarding data:

1. Operating systems must be maintained with vendor patches and updates.
2. Only approved software should be loaded. Unauthorized software, such as games and online download programs for music and video, are not permitted to be downloaded as this software can lead to the introduction of viruses, spyware and malware as well as negatively impact device performance.
3. Login passwords are required. Do not select "remember" password option.
4. Functional options not needed should be disabled such as a blue tooth.

PERSONALLY OWNED DEVICE POLICY

Purpose: The purpose of this document is to establish the statewide policy for the use of personally owned devices by authorized users on state owned and operated networks. This policy serves to protect state networks, applications and data.

Policy: Personally owned devices include, but are not limited to, desktops, laptops, printers, personal digital assistants (PDAs), smart phones, tablets and storage devices such as flash memory (memory sticks), flash cards, portable hard drives, MP3 players and other peripherals that may connect to a PC or laptop.

As the use of smartphones and tablets grow in popularity, the demand to use these devices in the workplace has significantly increased. This use, referred to as Bring Your Own Device (BYOD), provides mobile productivity advantages and increases user satisfaction. Several platforms have been implemented to support the use of BYOD devices in participating agencies while minimizing risk. These include:

1. A mobile device management platform to allow secure access to state email by creation of a secure container to separate business and personal data.
2. A guest wireless network that provides Internet access while at the same time prohibiting access to the State's data resources

The use of all personally owned devices must be approved by execution of the referenced Personal Device User Agreement. The Department of Information Technology (DoIT) will neither install nor provide support for any personal devices connected to state networks, with the exception of the creation of applicable accounts. Approved BYOD devices are still treated as personal devices and are not considered 'managed' with DoIT support.

The use of any personally owned device accessing state owned equipment/networks not specifically approved is prohibited unless authorized as noted above.

This policy applies to authorized users connecting to state networks in any manner, via a state-owned computer at their normal workspace or remotely via an Internet-provided Virtual Private Network (VPN) or dial-in. Access to state resources via a state-owned smartphone device must use secure VPN access. Devices should not be setup as MiFi (My Wi-Fi) hotspots which provide access by additional devices.

Accountability: All authorized users of any state and/or agency network shall adhere to this policy.

It is the responsibility of all agency heads or their designee to enforce this policy. Employees who do not comply with this policy shall be subject to disciplinary action as outlined in the Administrative Rules of the Division of Personnel.

Description: This policy serves to protect state networks from viruses and other potential security intrusions in addition to ensuring the security of confidential state data.

Reference: IT Standards Exception Policy
Personal Device User Agreement
Mobile Device Security Policy

PORTS AND SERVICES POLICY

Purpose: The purpose of this policy is to define the handling of ports and services at the state network edge via firewalls managed by the Department of Information Technology (DoIT).

Policy: Firewalls provide critical protection of state network resources. Firewall standards define the configuration, access and management requirements of firewalls based on the State's information security policies.

To strengthen the security posture of the state network, authorized ports and services for inbound and outbound traffic have been identified and documented in the referenced Ports, and Services Authorized List. Inbound and outbound traffic not expressly permitted by the firewall shall be blocked as unnecessary ports and services that expose the state network to external attack and contribute to unnecessary network traffic.

Applications rely on ports and services, so when developing new applications or planning for major application updates, developers must identify all ports and services required and comply with the authorized list to the extent feasibly possible. Ports and services required that are not on the approved list must have a functional and technical justification submitted for approval prior to the application and/or updates being put into production.

The Infrastructure Change Request (ICR) must contain the required ports and services along with the date of the approved request in the Secure Field on the ICR. ICRs without this information will not be approved.

Accountability: It is the responsibility of all agency heads or their designee to enforce this policy. Employees who do not comply with this policy shall be subject to disciplinary action as outlined in the Administrative Rules of the Division of Personnel.

Description: This policy serves to protect State network resources, systems and data.

Reference: Firewall Configuration Standards (internal)
Ports and Services Authorized List (formerly PCI Services and Ports Authorized List)
Ports and Services Request Procedure
Ports and Services Request Form
IT Standards Exception Policy

REMOTE ACCESS POLICY

Purpose: The purpose of this policy is to define standards for requesting remote access and utilization of the State's network resources. This policy applies to remote access connections used to conduct business on behalf of the State of New Hampshire, including application access, reading or sending e-mail and viewing internet/intranet web resources. This policy does not apply to publicly accessible State of NH websites, including those sites that support access to state resources such as e-mail.

Policy: Employees must request remote access from their immediate supervisor and receive agency approval from their Agency Head or designee and the Department of Information Technology (DoIT) Chief Information Officer (CIO). Access granted is for business use only.

Remote access includes requests for terminal services and Remote Desktop Protocol (RDP) used to access devices in a remote control manner. Users connecting remotely into Payment Card Industry (PCI) environments must utilize the designated Two Factor Authentication (TFA) solution along with the state provided VPN.

Remote access accounts will be issued only to individuals; generic and/or shared accounts are not allowed without an approved exception.

It is the responsibility of New Hampshire State employees, contractors, vendors and agents with remote access privileges to the State's network to ensure that their remote access connection is given the same consideration as the user's on-site connection. When remote access is no longer required, a request to remove the account must be submitted. Requests for non-state remote access must specify an account start and end date. For vendor access to PCI environments, accounts should be enabled only during the time period needed and accounts should be monitored when in use.

Remote access/VPN software must be kept in possession of the authorized user and cannot be distributed to any other person. Passwords must not be shared with anyone at the remote location, whether at home or while traveling.

Users must be physically present at the computer when remotely connected. If remote work is idle or the computer is left unattended, the user must exit and log out of all applications and disconnect the session. Computers should not be accessible by others. An inactivity timeout, as specified in the referenced configuration standards, is implemented.

When using dial-in to the State, the time spent connected must be limited to what is necessary as there is a per-minute charge for each minute connected to the phone line whether idle or not.

Remote access is only guaranteed to the extent that the State will ensure availability of the phone lines or the Internet components necessary for a VPN connection. The use of non-State-supplied equipment is not allowed. No support for the use of these devices will be provided.

Management staff can monitor remote access usage; monthly usage reports are common.

The Department of Information Technology (DoIT) has the right to revoke the privileges of the remote access account at any given time if this policy is violated.

SOFTWARE CONFIGURATION MANAGEMENT POLICY

Purpose: To establish a common and uniform policy regarding software and application configuration management documentation for all internal or external state developed software products where they are supported by the Department of Information Technology (DoIT) or contain state assets utilized in support or administration of DoIT business partners.

Policy: Software Configuration Management (SCM) involves identifying the configuration of the software (i.e., selected software work products and their descriptions) at given points in time, systematically controlling changes to the configuration through the use of version control and check-in/check out processes, and maintaining the integrity and traceability of the configuration throughout the software life cycle. This policy requires all new, changes and modifications to any existing software, application or code be recorded and handled in a consistent manner in a central repository managed by DoIT. The work products placed under SCM include the software products that are delivered to the customer (e.g., the Software Development Methodology (SDM) documentation and the software code) and the items that are identified with or required to create or manage these software products (e.g., the compiler).

Accountability: It is the responsibility of each Agency Head or designee to enforce this policy. Employees who do not comply with this policy shall be subject to disciplinary action as outlined in the Administrative Rules of the Division of Personnel.

Description: SCM is critical to ensure that all new, changes and modifications to any existing software, application or code is recorded and handled in a consistent manner.

Reference: Harvest Documentation Standard
Change Management Control Standards
ASD System Development Methodology (SDM)
IT Standards Exception Policy
Application Security Policy

FINAL

NHS - 12.06.2011 - v.7

USER ACCOUNT AND PASSWORD POLICY

This policy is not posted due to security concerns. If you would like to make a request to view the complete policy document, please e-mail DoIT-Security@doit.nh.gov.

WEB AND MOBILE APPLICATION ACCESSIBILITY POLICY

Purpose: To establish a common and uniform policy for all State of New Hampshire agencies to ensure that all web and mobile applications are accessible to disabled users.

Policy: All New Hampshire State agency web and mobile applications shall comply with Title II of the Americans with Disabilities Act, and be consistent in design and navigation with Section 508 of the Rehabilitation Act of 1973.

Accountability: This policy pertains to all State of New Hampshire agency web and mobile applications and to their administrators.

State agencies shall designate a staff member to be responsible for incorporation of this Policy. This responsibility includes the dissemination of guidelines, standards and compliance monitoring reports to the appropriate staff. Appropriate staff includes, but is not limited to, agency employees responsible for site administration or content development as well as any consultant or vendor responsible for an agency web or mobile application and/or content.

The Web Services Division (WSD) within DoIT will regularly monitor all agency web and mobile applications for Section 508 compliance and will send a monitor report to the agency staff member designated as responsible for the incorporation of this policy. It shall be the responsibility of the agency to ensure its web and/or mobile application is in compliance.

Employees who do not comply with this policy shall be subject to disciplinary action as outlined in the Administrative Rules of the Division of Personnel.

Description: The enactment of the Americans with Disabilities Act of 1990 (ADA) protects Americans with physical or mental disabilities from discrimination. There are five sections to the ADA: Employment, Public services, Public accommodations and services operated by private entities, Telecommunications and Miscellaneous provisions.

In 1998, Congress amended the Rehabilitation Act to require Federal agencies to make their electronic and information technology accessible to people with disabilities. Inaccessible technology interferes with an individual's ability to obtain and use information quickly and easily. The passing of Section 508 eliminates barriers in information technology, to make available new opportunities for people with disabilities and to encourage development of technologies that will help achieve these goals. This policy requires all state agencies to comply with Section 508 when they develop, procure, maintain or use electronic and information technology. Under Section 508 (29 U.S.C. § 794d), agencies must give disabled employees and members of the public access to information that is comparable to the access available to others.

Accountability: This policy pertains to all State of New Hampshire agency web sites and applications and to their administrators. State agencies shall designate a staff member to be responsible for incorporation of this Policy. This responsibility includes the dissemination of any additional guidelines, standards and compliance monitoring reports to the appropriate staff. Appropriate staff includes, but is not limited to, agency employees responsible for site administration or content development as well as any consultant or vendor responsible for an agency Web site and/or content.

WEB SITE PRIVACY POLICY

Purpose: To establish a common, uniform policy for all State of New Hampshire web sites regarding the privacy of personal information.

Policy: In the State of New Hampshire, laws exist to ensure that government is open and that the public has access to appropriate information obtained and held by the government. At the same time, the State recognizes that personal information collected by the State should be used only for the purpose for which it is collected. Except as authorized by law, such information will not be disclosed to other persons or organizations. Therefore, it is the policy of the State of New Hampshire that all personal information collected by state agency web sites shall be subject to the following principles:

- *Electronic information* - information collected and held electronically shall be afforded the same protection as non-electronic information;
- *Collection of personal information* - the collection of personal information shall be limited to and consistent with the requirements of the government program or activity;
- *Use of personal information* - individuals shall be informed as to why information is being collected and how it will be used;
- *Disclosure of personal information* - disclosure of information shall be limited to the purpose for which it was collected unless otherwise authorized by law; when practical and provided by law, information may be obtained from other government entities;
- *Access to personal information* - individuals shall be allowed a reasonable opportunity to obtain access to their personal information and to ensure that it is correct;
- *Security precautions* - reasonable precautions shall be taken to ensure the security of personal information.
- All state agency web sites shall provide information about the State of New Hampshire's Web Site Privacy Statement.

Accountability: This policy applies to all state agency web sites. It is the responsibility of each agency to enforce this policy.

Description: Web Site Privacy Statement information can be found at:
<http://www.nh.gov/disclaimer.html> including:

- Information about users the State of New Hampshire collects through its web sites
- Public Disclosure
- Cookies, Security, Disclaimer and Contact Information

WIRELESS ACCESS POLICY

Purpose: To establish a common and uniform policy regarding the acquisition, installation and use of wireless networks to access state network resources by state and non-state personnel.

Policy: Wireless is a method of communication without a physical connection. Wireless technologies can be used to communicate and transfer data to printers and other devices within buildings, in addition to providing connectivity for mobile devices. All wireless devices capable of transmitting data are governed by this policy. Wireless devices include personal computers, laptops, smart phones, Personal Digital Assistants (PDAs) and printers.

Wireless networks are not a replacement for wired networks. The purpose of wireless networks is to extend the wired network. Wireless networks have less bandwidth capacity than wired.

All devices capable of wireless communications, whether mobile or not, connecting to any state network from within or external to the state network, must be authorized by the agency head or designee. Wireless networks provided for staff and guests should not be used to transmit sensitive data, nor should they be connected to systems which transmit or hold sensitive data. Wireless access should be disabled when not required.

All Wireless Local-Area-Networks (WLAN) must be reviewed and approved by the DoIT prior to acquisition and installation. All WLAN installations must use approved hardware and software, comply with configuration standards, and be registered with the DoIT. Wireless Access Points (APs) and Base Stations are subject to periodic audits by the DoIT.

Wireless networks are prohibited within Payment Card Industry (PCI) environments. In the event a wireless network is authorized, it must be separated from the cardholder data environment by a firewall which must be configured to deny or control (if such traffic is necessary for business purposes) any traffic from the wireless environment into the cardholder data environment.

All wireless Network Interface Cards (NIC) purchased for use in state-owned laptops or desktop computers must meet the wireless NIC procurement standard and be authorized by the DoIT. All wireless NICs must use recommended security configurations. Wireless NICs are subject to periodic audits by the DoIT.

All wireless data connections to state network resources, whether internal or external, must be made via the agency approved and state-supplied secure Virtual Private Network (VPN) as specified in the Remote Access Policy. All wireless devices must use encrypted traffic and support a hardware address that can be registered and tracked. The use of unauthorized or unsecured wireless communication mechanisms to connect to state network resources is prohibited.

The wireless access user must comply with all applicable policies, including but not limited to those referenced below. They must immediately report to their manager any incident or suspected incidents of unauthorized access and/or disclosure of company resources, databases, networks, and any other related components of the organization's technology infrastructure. The wireless access user also agrees to and accepts that his or her access and/or connection to the State's networks may be monitored to record dates, times, duration of access, data types and volumes in order to identify unusual usage patterns or other suspicious activity. As with in-house computers, this is done in order to identify accounts/computers that may have been compromised by external parties.