NYS DEPARTMENT OF HEALTH
SECURITY REQUIREMENTS

1. INTRODUCTION

1.1.
All systems for the New York State Department of Health (NYSDOH) both internal and external must comply with the security requirements listed in this document.

Contractors and/or NYSDOH program area are required to work with the NYSDOH CISO (New York State Department of Health Chief Information Security Officer) to satisfy these requirements.

An acceptable Security Plan will be a mandatory project deliverable and must be completed prior to commencement of detailed application and systems development, unless otherwise approved by the NYSDOH CISO. The Security Plan must address the following components and be presented to the NYSDOH CISO for approval. The standard NYSDOH Security Plan template will be provided prior to commencement of the project.

Security Plan Components

1) **Secure Transmission**
2) **Systems and Network Security**
3) **Application Security Requirements**
4) **Data integrity,**
5) **Data availability**
6) **Account management**
7) **Security Incident Management and Audit Requirements**
8) **Proprietary Information, Copyright and Software Licensing**
9) **Data Confidentiality**

For management and maintenance of existing systems, NYSDOH CISO-approved security may already be in place for many of the security components required. Addressing gaps in these requirements within existing components will be the responsibility of the NYSDOH program area unless otherwise specified. Contractors and/or NYSDOH program area will have the responsibility to ensure new components are in compliance with the security standards in this document, as applicable.

Each project may not need to provide mechanisms for every security component, particularly if the proposed system/solution will leverage existing NYSDOH systems. NYSDOH program area, working in conjunction with the NYSDOH CISO as necessary, may make known in any RFP or project description which requirements will be managed by NYSDOH outside the scope of this project. Project proposals should describe measures to address all security requirements in this document in their Security Plan, as well as indicating which will be handled by NYSDOH program area and are therefore not applicable to the proposed solution.

For example, if a component of the systems network account management and authentication is accomplished using the NYSDOH Health Commerce System (HCS), which is a NYSDOH CISO-approved system, the network account management and authentication requirements are satisfied by NYSDOH and can be stated as such. If this is not the case a description of how authentication, along with how account management will be handled and what the approach will be regarding these requirements, must be included in the Security Plan.

1.2
When the application/system is hosted internally, i.e., within the network of NYSDOH, network and account management security policies will adhere to NYSDOH infrastructure as defined in Section 2.2.3 and Section 2.6 of this document. NYSDOH CISO performs vulnerability scans as required on internally hosted systems using standard approved tools. Vulnerabilities are expected to be corrected in a timely manner, with critical vulnerabilities fixed quickly. Contractors and/or NYSDOH program area will work with the NYSDOH CISO during security assessment, vulnerability fixes, and security testing.

NYSDOH web server capabilities are typically utilized if the systems and applications are hosted inside the NYSDOH network. This environment includes, but is not limited:

(a) Single-sign-on via NYSDOH "WAARP" SSO
(b) Ability to scale to large number of users
(c) Providing high-level data integrity
(d) Providing for basic security of the data at rest and in motion
(e) Built in audit capabilities
(f) Providing point in time recovery
(g) Providing back up and recovery capabilities
(h) Providing logging information for back up, recovery and auditing
(i) Providing support for large objects (blobs, etc)
(j) Providing support for clustering and load balancing
(k) Providing SSL connectivity
(l) Providing data confidentiality
(m) Providing data availability near 24/7/365 if required and requested
(n) Compliance with all NYSDOH security policies

NYSDOH project leads can obtain further details from NYSDOH Information Systems and Health Statistics Group (ISHSG) staff upon request.

The contractor and/or NYSDOH program area will work with NYSDOH ISHSG system and network staff to ensure adequate NYSDOH services and capabilities exist for the proposed system as required. NYSDOH program area will be responsible for funding additional services as needed and may pass this requirement to contractors.

1.3
When the systems (databases, files, data, networks, and/or applications) are hosted outside NYSDOH network (i.e., hosted externally), all requirements detailed below must be satisfied:

1.3.1. Ensure network and host security is defined and in accordance with NYSDOH Network Configuration Policy (Section 2.2.3).

1.3.2 Documentation must exist in the form of schematics and / or diagrams of the network layout of the system in accordance with the Network Configuration Policy and a description of how security will be performed. This network plan must be submitted for review and approval to NYSDOH CISO during development and again just prior to production. This should include diagrams with servers clearly labeled. The plan should clearly explain the system's networking security policy (which can be included as an appendix to the Security Plan), and should clearly describe how vulnerability scans and other on-going security measures will be implemented including frequency of security measures and tests.

1.3.3. NYSDOH CISO must approve the design. Details of all components of the system and all security components must be reviewed by NYSDOH CISO.

1.3.4. Any changes to the approved network layout must be reviewed and approved by NYSDOH CISO for continued compliance with NYSDOH network standards.

1.3.5 Documentation must be submitted to NYSDOH CISO for review and approval of how sessions are established.

1.3.6. Assurance must be provided that when user sessions for an application or network connection terminate, either normally or abnormally, all related network sessions will also terminate.

1.3.7. Assurance must be provided that the network is eavesdrop-proof through the use of

technologies including but not limited to secure hubs and/or switches. Wireless networks must use WPA2 or higher encryption, they must not broadcast SSIDs and they must ensure only authorized hosts can connect to the WLAN. Wireless may not be used for secure private e-commerce or external-class networks as defined in the Network Configuration Policy (Section 2.2.3).

1.3.8. Assurance must be provided that the information, including system(s) will be isolated from other networks via secured network devices such as firewalls and/or state-full routers, including but not limited to other technologies that allow such isolated networks.

1.3.9. Assurance must be provided that devices to be used are protected by packet-filtering firewalls and/or firewall-grade routers.

1.3.10. Assurance must be provided that all devices are operated utilizing robust operating systems and hardened against attack. Hardening includes and is not limited to OS patch management, software patch management and removing unnecessary services where applicable. Systems should comply with New York State Cyber Security Policy P03-002 defined at http://www.cscic.state.ny.us/lib/policies/documents/Cyber-Security-Policy-P03-002-V3.2.pdf and National Institute of Standards and Technology (NIST) standards defined at http://csrc.nist.gov/publications/PubsSPs.html, such as:

NIST SP800-12 (An Introduction to Computer Security: The NIST Handbook)
NIST SP800-14 (Generally Accepted Principles and Practices for Securing Information Technology Systems)
NIST SP800-27 (Engineering Principles for Information Technology Security)
NIST SP800-40 (Creating a Patch and Vulnerability Management Program)
NIST SP800-41 (Guidelines on Firewalls and Firewall Policy)
NIST SP800-44 (Guidelines on Securing Public Web Servers)
NIST SP800-50 (Building an Information technology Security Awareness and Training Program)
NIST SP800-53 (Recommended Security Controls for Federal Information Systems)
NIST SP800-54 (Border Gateway Protocol Security)
NIST SP800-61 (an Introductory Resource Guide for Implementing the HIPAA Security Role)
NIST SP800-70 (National Checklist Program for IT Products-- Guidelines for Checklist Users and Developers)
NIST SP800-81 (Secure Domain Name Systems (DNS) Deployment Guide)
NIST SP800-88 (Guidelines for Media Sanitization)
NIST SP800-92 (Guide to Computer Security Log Management)
NIST SP800-94 (Guide to Intrusion Detection and Prevention Systems (IDPS))
NIST SP800-95 (Guide to Secure Web Services)
NIST SP-800-123 (Guide to General Server Security)

1.3.11. Assurance must be provided that periodic network vulnerability scans and tests be performed. These scans and/or tests should include and not be limited to open ports scans and network intrusion detection. This requirement must be addressed within the Security Plan, and the plan will be reviewed by NYSDOH CISO. For externally hosted systems, specify tools that will be used for vulnerability scans in the security assessment section. Within NYSDOH managed (internally hosted) networks, standard tools are used in systems like the Health Commerce System (HCS), and these tools were approved by NYSDOH CISO. Similar standard tools must be used for scanning in externally hosted systems as well, and these tools will be reviewed for acceptability by NYSDOH CISO. After review, NYSDOH CISO must approve the tools that are planned to be used for vulnerability scanning. Contractors can request of NYSDOH the names of the scanning tools used in NYSDOH internally hosted applications/systems, if required.

NYSDOH CISO reserves the right to run periodic vulnerability scans and review reports from scans as needed. Scans and tests will be performed prior to being implemented on production networks and after software of operating systems or configuration changes are made. All source code must be provided for periodic review by NYSDOH CISO. Critical vulnerabilities identified during scans must

be fixed and all NYSDOH CISO's security recommendations must be followed. Scans and tests must be performed at least annually and more frequently for critical and/or high-risk systems, such as those exposed to external users and/or the Internet. Scan frequencies should be defined within the scope of work.

1.3.12. All hardware, networking components, physical devices and software related to the project/system are to be protected and no unauthorized person should be able to access these hardware and software components. Any intrusion and unauthorized accesses must be stopped and reported to the NYSDOH CISO as they occur.

1.3.13. Description and documentation must exist of the steps to physically secure the location of servers or workstations that will contain applications, source code and/or databases related to the project/system. This must contain how all these physical devices are protected.

1.3.14. Description and documentation must exist regarding disaster recovery/business continuity of the systems. Periodic back-ups of data, databases, software, applications including and not limited to source code of anything defined within the project scope must be performed according to the disaster recovery/business continuity requirements. Encryption of backup media is encouraged and at times may be required by law.

1.3.15. Systems hosted outside NYSDOH-managed networks, including all hardware, software, networking components, applications, data, etc, must have the same level of security as that of systems hosted within NYSDOH networks. Some of the capabilities of servers hosted internally are highlighted in Section 1.2. Periodic reviews and keeping externally hosted systems up to date to meet all security requirements are required. Working with NYSDOH CISO to ensure that externally hosted systems are at least as secure as NYSDOH-internally hosted systems is required. NYSDOH CISO reserves the right to review externally hosted systems to ensure they satisfy NYSDOH security requirements completely.

1.3.16. Periodically NYSDOH may update security policies pertaining to systems hosted externally. NYSDOH will make updated standards and polices available.

2. SECURITY REQUIREMENTS

2.1 SECURE TRANSMISSION

The following requirements need to be followed whenever computer systems are used and data is transmitted electronically.

2.1.1. All information transfers must be secure from point to point as outlined in this section commensurate with data.

2.1.2. No sensitive or confidential information, current, historical, archived files or other information, will be allowed via unencrypted channels.

2.1.3 Information transmission must be commensurate with sensitivity and confidentiality of the data. This secure transmission policy applies to all sensitive and confidential information and the Security Plan must include details on how secure transmission is addressed.

2.1.4. Appropriate measures to protect information during transmission must be in place. These include but are not limited to: use of data encryption, and/or using transmission headers, checksums, digital signatures and control totals.

2.1.5. Assurance must exist in the Security Plan that information classified as "confidential" (as defined in an RFP, HIPAA, NYSDOH policies related to data classification, and/or other NYS Laws and Regulations) must not be transmitted across an open or insecure network unless it is encrypted.

2.1.6. Encryption implementations must be approved by NYSDOH CISO before being utilized. The management of encryption keys and mechanisms must be planned and must conform to NYSDOH standards of encryption management agreed upon with NYSDOH CISO.

2.1.7. Proprietary encryption algorithms used will provide supplemental security only and will not be the sole source of encryption security. All information stored is to be encrypted using above average encryption strength (currently 128-bit for data in motion) except where the information is required for basic system operation and encryption beyond industry-standard levels is not available.

2.2 SYSTEMS AND NETWORK SECURITY

2.2.1 Server Requirements

Security requirements for server(s) used for the project/system are included but not limited to what is outlined in this section.

All information must be stored on appropriately secured servers, as required in Section 2.2.3, Network Configuration Policy, and they need to have appropriate level of access control.

Systems used for NYSDOH systems must have appropriate physical controls and be described in the Security Plan.

NYSDOH uses and maintains anti-virus software to ensure virus and anti-malware protection steps are in place to ensure safe operation of the network(s). The approach used should be included in the Security Plan. NYSDOH CISO reserves the right to review the virus protection solution and make recommendations to ensure proper virus protection/prevention.

2.2.2 Remote Access Control

2.2.2.1. All systems and applications that connect remotely to NYSDOH systems or networks used by NYSDOH systems, whether hosted internally or externally, must be approved in writing by NYSDOH CISO.

2.2.2.2. All remote access must be logged at all times, including the ability to produce documentation and justification for any lapses in logging.

2.2.2.3. The use of modems attached to any permanently network-connected device is not allowed unless approved in writing by NYSDOH CISO.

2.2.3 Network Configuration Policy

An organization or Internet domain may contain several types of networks. Each type of network provides different methods of risk reduction, depending on the network access needs. Below is a basic definition of acceptable network configurations.

2.2.3.1 All Networks

- Eavesdrop-proof through use of secure hubs and/or switches
  (See NIST SP800-41, SP800-53, SP800-94)
- Isolated from other networks via secured network devices such as firewalls and/or state-full routers
  (See NIST SP800-41, SP800-53, SP800-54)
- Logging of all successful and failed attempts should occur at all network perimeter devices
  (See NIST SP800-53, SP800-92)
- Logs should be stored on protected hosts

(See NIST SP800-92)

- Logs should be reviewed at least every business day
- Hosts must comply with security modules as described in: NIST SP800-53, -41, -44, -92, -94, -95, and -123
- Network users and administrators must receive security awareness training (See NIST SP800-12, NIST-SP800-50)

2.2.3.2 Untrusted Networks

Definition: A network outside of the direct, immediate control of the organization.
Example: Internet

Requirements:

- Only firewalls and/or firewall-grade router devices should reside on an untrusted network
- Management of devices on an untrusted network must be via a trusted connection to the device

2.2.3.3 External Networks

Definition: servers that require unauthenticated access from untrusted networks, such as the Internet.
Example: Network containing public web or mail servers

- No client (user) machines should reside on an external network
- Devices should be protected by packet-filtering firewalls and/or firewall-grade routers
- Devices must run robust operating systems and be hardened against attack. Hardening includes loading of all applicable patches as they are released and removing unneeded services
- No confidential or sensitive information may be stored, either temporarily or permanently, on any devices on this network except as needed for fundamental system operation and then only if encrypted (/etc/shadow, for example)
- Network logs should be archived for a least six (6) months
- Application logging should be activated wherever possible and reviewed at least every business day
- Inbound and outbound connectivity should be limited to needed services****** but may go to and come from any type of network
- Authentication systems must be centrally managed

2.2.3.4 E-commerce Networks

Definition: Servers that provide authenticated access from untrusted networks, such as the Internet.
Example: Networks used to transact confidential information with clients and/or partners

- No client (user) machines should reside on an e-commerce network
- Devices should be protected by packet-filtering firewalls and/or firewall-grade routers
- Devices must run robust operating systems and be hardened against attack. Hardening includes loading of all applicable patches as they are released and removing unneeded services
- Network logs should be archived for a least six (6) months
- Application logging must be activated where ever possible and reviewed at least every business day
- Confidential or sensitive information stored on devices in this network must be secured independently from network access security control (for example, separate password files) where ever possible
- Confidential or sensitive information stored on devices in this network must be encrypted using above-average encryption strength (currently 128-bit) except where the information is required

for basic system operation and encryption beyond industry-standard levels (currently 56-bit) is not available (example: /etc/shadow)

- Confidential or sensitive information transferred to or across untrusted networks must be encrypted
- System and application standards designed to protect the systems, applications and network must be established by the system administrators
- Access to systems must be limited to needed parties and must be approved, where applicable, by data owners
- Inbound and outbound connectivity should be limited to needed services**
- Inbound connectivity from untrusted networks must be authenticated. Authentication must be encrypted to industry-standard levels (at least 56-bit at time of writing)
- Authentication systems must be centrally managed

2.2.3.5 Private Networks
Definition: Internal network which hosts users and internal-only applications and servers
Example: Corporate intranet

- Devices should be protected by packet-filtering firewalls and/or firewall-grade routers
- Devices should be maintained in a secure state
- An automated virus-protect solution must be in operation
- Network logs should be archived for a least six (6) months
- Application logging should be activated wherever possible and frequently reviewed by the individual(s) responsible for the application
- Access to systems must be limited to needed parties and must be approved, where applicable, by data owners
- No inbound connectivity from untrusted networks is permitted
- Inbound connectivity from e-commerce networks is permitted provided the private network devices run robust operating systems and hardened against attack. Hardening includes loading of all applicable patches as they are released and removing unneeded services. The needed services cannot provide access beyond the scope of the need **
- Outbound connectivity should be limited to only to needed services**
- Authentication is required for access to confidential or sensitive information. This includes information temporarily or permanently stored on PCs or other single-user devices

2.2.3.6 Secured Private Networks
Definition: Servers that hold the organizations most sensitive information and are secured from all other types of networks
Example: Network containing database servers containing credit card or patient-identifying data

- No client (user) machines should reside on a secured private network
- Devices should be protected by packet-filtering firewalls and/or firewall-grade routers
- Devices must run robust operating systems and be hardened against attack. Hardening includes loading of all applicable patches as they are released and removing unneeded services
- Network logs should be archived for a least six (6) months
- Application logging must be activated where ever possible and reviewed at least every business day
- Confidential or sensitive information stored on devices in this network must be secured independently from network access security control (for example, separate password files) where ever possible
- System and application standards designed to protect the systems, applications and network must be established by the system administrators

- Access to systems must be limited to needed parties and must be approved, where applicable, by data owners
- Inbound and outbound connectivity should be limited to needed services**
- No inbound connectivity from or through untrusted networks is permitted
- Authentication systems must be centrally managed

2.2.3.7 Recommended Best Practices

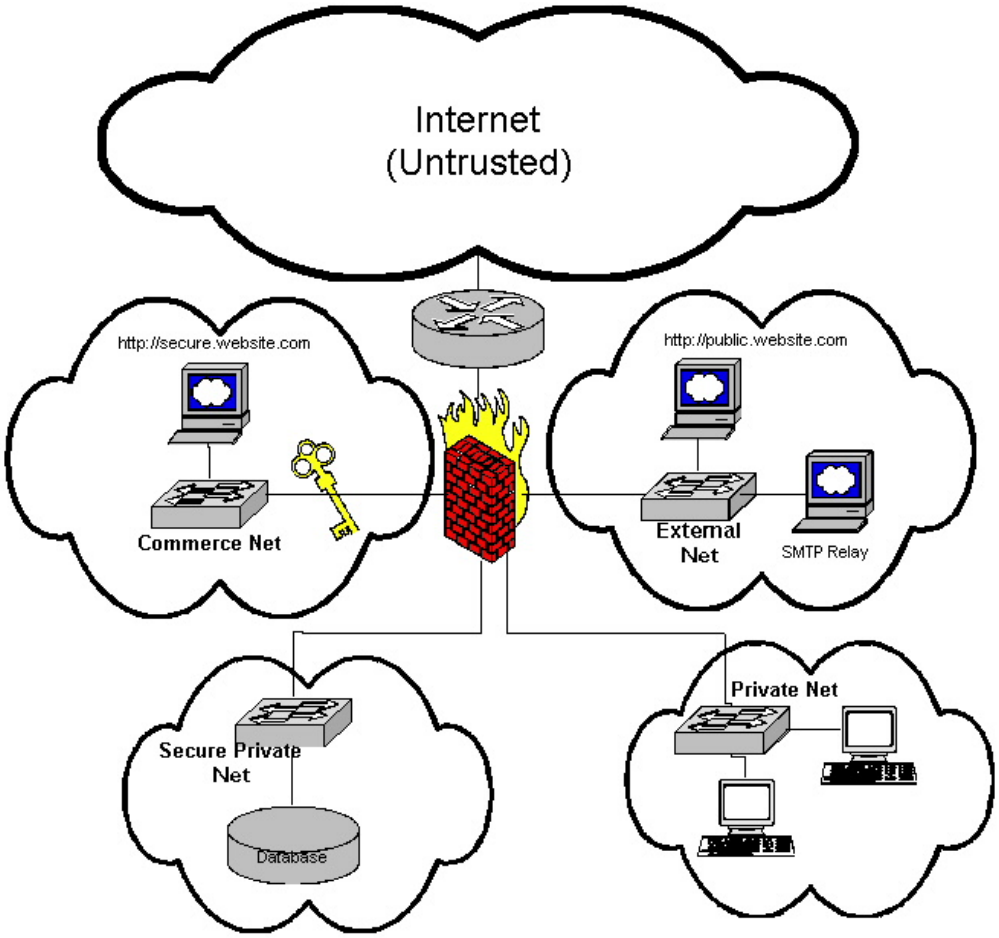
- Network Intrusion Detection Systems be deployed at strategic locations
- Network Mapping/Scanning be done at regular intervals to detect vulnerabilities

NYSDOH Auditing

- Network administrators must provide written confirmation of policy compliance prior to full production implementation and quarterly thereafter. This attestation must be supported by detailed network descriptions, which address the related policy aspects
- NYSDOH Security Office will be provided secure shell (SSH) access to at least one device in each network. The account must have privilege to create network sockets
- NYSDOH Security Office reserves the right to conduct on-site inspection of network infrastructure for the purpose of policy compliance verification
- Modifications to these auditing requirements may be negotiated but should not be assumed

** **DOH Security Unit will perform the risk benefit analysis prior to approval and deployment of services**

NYSDOH Network Configuration Policy Diagram



2.3 APPLICATION SECURITY REQUIREMENTS

Systems and application development must comply with NYSDOH security policies outlined in this document. When new application code is developed, the security within the Software Development Life Cycle (SDLC) methodology must be documented. The NYSDOH CISO reserves the right to review the development plan and may apply additional requirements for promotion of applications.

NYSDOH CISO review and approval do not apply to emergency code fixes that need to be done during production emergencies, however NYSDOH program area staff is required to notify the NYSDOH CISO immediately when emergency fixes are applied and must work to correct any vulnerabilities discovered in these updates in a timely manner. Any new or updated application code is still expected to go through NYSDOH CISO periodic application security scanning and vulnerabilities must be corrected as specified by NYSDOH CISO in consultation with NYSDOH management.

Applications will be scanned for security vulnerabilities by NYSDOH CISO. Periodically, the NYSDOH CISO may request a copy of the current software source code for its own internal security testing, archiving or other purposes. The contractor/NYSDOH program area is expected to work with the NYSDOH CISO to manage security assessment and fix critical vulnerabilities that may jeopardize the security of the system.

2.3.1. Testing
Application security tests, reviews and audits must be conducted regularly to evaluate the security of systems and applications. Applications must be tested for vulnerabilities prior to promotion to production. Issues must be identified and rectified as found. When changes are made to related software or applications, testing will be performed again to ensure NYSDOH compliance.

2.3.1.1. The Security Plan must describe the proposed security testing procedures and include responsibilities for security testing. Contractors/NYSDOH staff working with systems on NYSDOH-managed networks are encouraged to use the source code analysis and application security scanning tools managed by the NYSDOH CISO, but may specify alternatives. Alternatives must be approved by NYSDOH CISO.

2.3.1.2. The Security Plan must include the external application testing platforms, if currently in use, as well as software source code testing platforms that are used.,

2.3.1.3. Use of live data for testing purposes: At no time should any application testing be performed on live data. Where ever possible, testing should be created to mimic live data but not contain any live information. Simulation of live data is suggested.

2.3.2. Application vulnerability areas include the following and must be addressed in the Security Plan as applicable.

2.3.2.1. Input Validation: ensure that all input validation be achieved in a manner to prevent any malicious requests or code from being processed.

2.3.2.2 Output Validation: ensure that all data retrieved from inter process operations has been appropriately validated.

2.3.2.3. Type Checking: Ensure that all data retrieved from inter process operations, including screen input, has been validated for the expected data type.

2.3.2.4. Bounds Checking: ensure that all variables be bounded by the length they are designed to be. This is a critical and integral part of Input Validation.

2.3.2.5. Writing Directly to a File: ensure that at no time any sensitive information be written to any external files (text or otherwise) except to log files, unless approved by the NYSDOH CISO. This

includes sensitive information and includes any external files used within the application on a temporary basis.

2.3.2.6. URL Passed Variables: ensure that variables will not be passed via a URL or are subjected to a high standard for Input Validation. Wherever possible, internal session variables should be used and only session reference given.

2.3.2.7. Caching SSL Pages: ensure all feasible precautions are taken to ensure that any cached SSL pages be removed upon exiting of the browser and/or the website.

2.3.2.8. Hidden Form Variables: ensure use of hidden form fields is limited; treat these fields with the same limited trust as other form fields and validate data provided in these fields as such.

2.3.2.9. Cookies: ensure that any cookies required for any and all web based applications will expire upon completion of the application. No cookies should be allowed to remain for an indefinite period of time. A Maximum Auth Cookie timeout will be required. Cookie values received from the client should be validated as with all other input. Authorization cookies must have an expiration time and comply with NYS Cyber Security Policy P03-002.

2.3.2.10. Tool Sets and External Code: Use of third-party modules and/or programs should be limited to items that are known to have undergone thorough security testing. Where possible, source code for any third-party solutions should undergo secure code reviews, including application scanning. No applications or modules should call or access external links or resources, unless this is part of the system's core functions. (For example, if the system is designed to call an external web service and process the result, external reference would be expected. Modules should not reference to external libraries for internal execution, however.) Likewise, no applications or modules should display external links unless this is part of the system's core functions. Use of code, modules and/or programs obtained from external sources must be in compliance with licenses agreements.

2.3.2.11. Configuration Files: ensure that no external configuration files will contain sensitive information including but not limited to clear-text user names and/or passwords. Encrypted configuration files and/or use of encrypted values within clear-text files are permitted.

2.3.3. Application Logging: Logs should be reviewed for application security at least each business day and critical issues should be escalated as required by NYSDOH policy and procedures and/or other applicable legal requirements.

2.3.4. Databases: ensure that all connections to any and all databases be secure, including but not limited to restricting connections to said databases from authorized applications, hosts, networks and users.

2.3.5. Database Queries: ensure that all database queries are secure, run by authorized users and application(s). Queries should be stored procedures wherever possible. At no time should input data be passed to the database without appropriate validation.

2.3.6. Writing to Screen including error messages: ensure all feasible precautions are taken to ensure that all error messages are benign and reveal no extra systems information. This includes abend or stack trace errors or any other information displayed that could be used in a malicious way against an application or system. A generic error message should be used at all times.

2.3.7. NYSDOH encourages scanning application source code for security vulnerabilities on a regular basis and addressing vulnerabilities as discovered. Critical findings are expected to be addressed on a regular/ongoing basis.

2.3.8. NYSDOH CISO will conduct periodic reviews of adherence to application security policies, test

procedures, guidelines and standards. The NYSDOH CISO and the contractor/NYSDOH program area will work together towards achieving as vulnerability free an outcome of the scan as possible.

2.3.9. All applications must be tested for vulnerabilities prior to promotion into production. Results must be cleared with NYSDOH CISO. NYSDOH CISO approval is required prior to promotion into production.

2.4. Data Integrity

Data integrity is an integral part of any application or system. The Security Plan must include specific details related to preserving the integrity of data maintained in the system.

No unauthorized person or process shall be allowed to update data or in any way impact data integrity. Account management requirements should be satisfied completely. Account management is detailed in Section 2.6.

The following should be explained in the Security Plan:

2.4.1. Explain how the integrity of all information sources within the scope of this system is maintained.

2.4.2. Explain how authorization required for all production system input is accomplished and tracked as appropriate.

2.4.3. Explain how the system is free from risks of undetected changes.

2.4.4 Explain how integrity of data is maintained on network systems. For internally hosted (NYSDOH) systems, NYSDOH runs periodic network scans and tests to help ensure the integrity of data and network systems.

2.4.5 Explain how a secure environment for the Source Code of any software will be maintained.

2.4.6. Explain how the risks that data input could contain malicious exploits, such as file uploads, will be detected, mitigated and handled.

2.5. Data Availability

Data must be available to the degree specified in the project requirements. The Security Plan must clearly describe the plan for ensuring Business Continuity, Disaster Recovery and Data Availability and the requirements/needs around each.

Data should be recoverable from backups when required. Measures must be in place to mitigate data loss. The Security Plan must specify the backup requirements, who is responsible for each component, how this will be achieved and how it will be verified, including the transfer of recent copies of backups to a physically and environmentally secure off-site storage location, if applicable.

Backup procedures and practices should be monitored regularly and any back up failures should be corrected immediately. Testing the backups should be done regularly to determine if data files and programs can be recovered. All recovery of information from back up and restoration procedures should be documented and appropriate staff well trained for executing successful recoveries during disasters and during situations of data loss.

Backup procedures and practices must comply with all security requirements included in this document, including data integrity and security of data transmission and access controls.

2.6. Account Management

Account management must be described in the Security Plan. This must address the requirements listed below which are found in NYS Cyber Security Policy P03-002 Part 10, Access Control Policy. This can be found at http://www.cscic.state.ny.us/lib/policies/documents/Cyber-Security-Policy-P03-002-V3.2.pdf. NYSDOH CISO reserves the right to review and approve the account management process.

Data systems hosted within NYSDOH's networks and made available to external entities must utilize the NYSDOH's existing account systems for at least primary authentication unless explicitly approved by NYSDOH CISO. Data systems to be hosted outside the NYSDOH's networks are encouraged to use these systems as well, however details must be included in the Security Plan to secure the inter-network communications and ensure security of this configuration. Contractors and/or NYSDOH program area are welcome to use additional authentication and/or authorization controls but must document the need for such and provide details related to account management as described in this section. Access management systems different from standard approved NYSDOH systems, such as Healthcom Commerce System (HCS), must be reviewed and approved by the NYSDOH CISO.

2.6.1. Access to NYSDOH information systems residing within NYSDOH networks (internal) and networks outside NYSDOH networks (external) must be managed to preserve the properties of integrity, confidentiality and availability. NYSDOH's information assets will be protected by appropriate logical and physical access control mechanisms commensurate with the value, sensitivity, consequences of loss or compromise, legal requirements and ease of recovery of these assets.

2.6.2. Information owners are responsible for determining who should have access to protected resources within their jurisdiction, and what those access privileges will be (read, update, delete, etc.). These access privileges will be granted in accordance with the user's job responsibilities. Workforce members must not be allowed access to NYSDOH information systems until properly authorized.

2.6.3. Only appropriate information owners or their delegates will make authorized requests for the registration and granting of access rights for personnel onto NYSDOH systems. As such, information owners and delegates must be formally designated, approved by management and documented. NYSDOH CISO reserves the right to review the authorization process implemented.

2.6.4. A user management and access tracking process shall be established and documented to outline and identify all functions of user management Standards and procedures must exist for account management in accordance with NYS Cyber Security Policy P03-002 which include:

a. Account provisioning, updating, de-provisioning and distribution (including, user identity verification, enrolling new users, deleting users and reviewing users)
b. Authorization assignment and revocation
c. Privileged account management (including granting, removing and periodic review)
d. Authentication token (such as password) management (including reset) and distribution, including user identification procedures
e. Access by third parties, such as sub-contractors, and vendors

2.6.5. Privileged user-ids must not give any indication of the user's privilege level, e.g., supervisor, manager, administrator. These individuals should also have a second user-id when performing normal non-privileged business activities, such as, accessing the email system. Where technically feasible, default administrator accounts must be renamed, removed or disabled. The default passwords for these accounts must be changed if the account is retained, even if the account is renamed or disabled.

2.6.6. For applications that interact with individuals that are not employed by NYSDOH, the information owner is responsible for ensuring an appropriate user management process is implemented. Standards for the registration of such external users must be defined and include the credentials that must be provided to prove the identity of the user requesting registration, validation of the request and the scope of access that may be provided. These standards will be reviewed and approved by NYSDOH CISO. Guidelines given in "Identity and Access Management: Trust Model" (found at http://www.cio.ny.gov/Policy/G07-001/G07-001.pdf) should be followed.

2.6.7. Logon banners are implemented where that feature exists to inform all users that the system is for NYSDOH business or other approved use consistent with NYSDOH policy, and that user activities may be monitored and the user should have no expectation of privacy. Logon banners are usually presented during the authentication process.

The standard approved NYSDOH banner is "Use of NYS Department of Health computers and related resources is restricted solely to the conduct of NYSDOH business. User IDs and passwords assigned to an individual are the responsibility of that individual and may not be shared with others. Compromise of user IDs and passwords to department computers must be immediately reported to NYSDOH CISO. Personal and unauthorized usage is prohibited unless stated otherwise by NYSDOH policy." Where not technically feasible due to length, the following legal notice may be used: "NYSDOH use only and subject to monitoring".

If possible, the notice should appear prior to authentication. If this is not possible, the notice should appear immediately after authentication.

2.6.8. Password Management

2.6.8.1. Passwords are a common means of authenticating a user's identity to access an information system or service. Password standards must be implemented to ensure all authorized individuals accessing NYSDOH resources follow proven password management practices. These password rules must be mandated by automated system controls whenever possible unless explicitly approved otherwise by NYSDOH CISO. These password best practices include but are not limited to:

a. passwords must not be stored in clear text;
b. use passwords that are not easily guessed or subject to disclosure through a dictionary attack;
c. passwords must be kept confidential and not shared;
d. passwords must be changed at regular intervals with a maximum expiration of 90 days;
e. change temporary passwords at the first logon;
f. when technology permits, passwords must contain a mix of alphabetic, numeric, special, and upper/lower case characters and be a minimum of 8 characters;
g. do not include passwords in any automated logon process (e.g., stored in a macro or function key, web browser or in application code)

2.6.8.2. To ensure good password management, password standards must be implemented on all platforms when technically feasible. Contractor and/or Program Area's adherence to password management practices will be reviewed by NYSDOH CISO.

2.7 Security Incident Management and Audit Requirements

NYSDOH CISO reserves the right to review, evaluate and audit for security compliance any component of the system to assess if security requirements are being followed. NYSDOH CISO reserves the right to coordinate and/or conduct security assessments and will discuss outcomes of security scanning with the contractor and/or program area to work towards fixing critical security vulnerabilities.

The Security Plan will include specifics on the approach of how these audit requirements will be accomplished taking into account items listed below:

2.7.1. System Logs must be available for the NYSDOH CISO to review and/or document how these will be reviewed on a periodic, ongoing basis.

2.7.2. Logs must be reviewed and documented every business day at least once every 24 hours. Assurance must be provided to certify the system is in conformance to Section 2.2.3 NYSDOH Network Configuration Policy of this document.

2.7.3. Systems must be monitored and when thresholds of specific security related events are reached NYSDOH must be notified. All suspicious or unusual events will be reported to the NYSDOH program area who will in turn notify the NYSDOH CISO of possible security incidents within 24 hours of discovery. The approach towards meeting the addressing of the requirement to monitor and detect security events and to execute proper responses to those events should be included in the Security Plan for review and approval.

2.7.4. Security Systems must be in place to record all security related events in an audit log. Where applications maintain their own authentication and/or authorization controls, the application must also maintain its own logs of authorized access privileges and unauthorized attempts at access. Account management requirements, outlined in Section 2.6, need to be followed. Typically these events include:

a) Valid and invalid user authentication attempts
b) Log on and activity of privileged users
c) Successful access to security system details
d) Access to resources outside normal hours
e) Changes to user security profiles
f) Changes to access rights of resources
g) Changes to system security configuration

2.7.5. Audit logs including logging analysis tools, systems and outputs, must be managed and stored in a secure manner to ensure their integrity. No unauthorized access should be permitted. At no time should anyone have access to change a log file. No logs may be altered in anyway.

2.7.6. All Security Logs should be archived for at least six (6) months, unless directed by other laws and/or regulations.

2.7.7. All users and administrators who are in relation to the scope of work for this project/system must receive periodic security awareness training and be qualified to work in a secure environment. Any updates to NYSDOH security policies should be communicated to these users and administrators.

2.7.8. All logs are to be made available to NYDOH CISO on an as needed or predetermined schedule for review.

2.7.9. A list of what software used in components of the system needs to be maintained and provided as required by NYSDOH CISO. NYSDOH CISO reserves the right to audit and review lists of software added and inspect code and assess compliance of security requirements. NYSDOH CISO may require code found to cause significant risk to NYSDOH be removed.

2.8 Proprietary Information, Copyright and Software Licensing

2.8.1. Software licenses must be reviewed on a periodic basis and the results must be reported to NYSDOH CISO to ensure that the terms of software licenses are being complied with.

2.8.2. Any unauthorized software is to be isolated and access disabled.

2.8.3. Appropriate licenses for any products provided as part of this project/system must exist. Licenses purchased under a contract are owned by NYSDOH.

2.8.4 Copying licensed or NYSDOH proprietary software must be limited to legitimate backup processes. NYSDOH will hold individual program areas and/or contractors liable for any inappropriate software use, distribution or license violations.

2.8.5. Any software including software developed, maintained, acquired or in any other way created during the length of this project is the expressed property of the NYSDOH and can not be used for any other reason than its intended use without prior approval of NYSDOH.

2.8.6. Contractors and/or external parties will return to NYSDOH any all material developed as part of this and any related projects/contracts at the conclusion of work on NYSDOH funded solutions. This would include removing any copies of NYSDOH-funded solutions or NYSDOH-proprietary data and/or information. NYSDOH Secure Disposal policies must be followed to ensure secure removal of said information.

2.8.7. Especially in the case of sensitive or confidential information, Contractor will ensure that all information at the expiration of this contract will be destroyed and documented as such. Documentation is to be supplied after all information is handed back to the NYSDOH and or subsequent contractor(s). NYSDOH APPM 430.0 Secure Disposal or Reuse of Media Policy must be followed.

2.8.8. All media, not owned and maintained by NYSDOH, must be securely erased or rendered unreadable before disposal as approved by NYSDOH CISO. Storage media must be sanitized at or above US Department of Defense standards at the end of contract after information is migrated to the NYSDOH and or the successor of the contract.

2.9 Data Confidentiality

The Security Plan must provide data confidentiality and integrity assurances through technologies including but not limited to field-level encryption, file level encryption and/or strong ACL controls. Information stored is to be encrypted using above average encryption strength (with 1024-bit or above) except where the information is required for basic system operation and encryption beyond industry-standard levels is not available.

3. Updates to Policies

The standards, guidelines and policies described in this document will be revised periodically. Changes to policies will be included in change management or during re-bid. NYSDOH will make notification of updates and changes to security policies.

References:

1. NYS Cyber Security Policy P03-002 at http://www.dhses.ny.gov/ocs/resources/documents/Cyber-Security-Policy-P03-002-V3.4.pdf
2. Health Insurance Portability Accountability Act (HIPAA)
3. National Institute of Standards and Technology Computer Security Resource Center at http://csrc.nist.gov/