|  |  |  |
|---|---|---|
| **<Organization Name>** | **Information Security System and Services Acquisition Policy** |  |
| Department Name | Policy # | **Issue Date:**<br>September 13, 2013 |
| Approved by: |  |  |

## 1. Purpose

<Organization Name> <Insert Organization Mission Here>. This policy establishes the Enterprise System and Services Acquisition Policy, for managing risks from third party products and services' providers, through the establishment of an effective third party risk management program. The third party risk assessment program helps <Organization Name> implement security best practices with regard to Systems and Services Acquisition.

## 2. Scope

The scope of this policy is applicable to all Information Technology (IT) resources owned or operated by <Organization Name>. Any information, not specifically identified as the property of other parties, that is transmitted or stored on <Organization Name> IT resources (including e-mail, messages and files) is the property of <Organization Name>. All users (<Organization Name> employees, contractors, vendors or others) of IT resources are responsible for adhering to this policy.

## 3. Intent

The <Organization Name> Information Security policy serves to be consistent with best practices associated with organizational Information Security management. The intent of this policy is to establish a method that will be used to evaluate third party services which host <Organization Name> Information and third party products which are procured to process <Organization Name> information, for information security risks.

## 4. Policy

<Organization Name> has chosen to adopt the System and Services Acquisition principles established in NIST SP 800-53 "System and Services Acquisition," Control Family guidelines, as the official policy for this domain. The following subsections outline the System and Services Acquisition standards that constitute <Organization Name> policy. Each <Organization Name> Business System is then bound to this policy, and must develop or adhere to a program plan which demonstrates compliance with the policy related the standards documented.

- SA-1 Best Practices: All <Organization Name> identified systems and services for procurement should be reviewed against best practices and standards for the technology type or service being acquired.
- SA-2 Capital Planning: All <Organization Name> Capital planning activities, which include the acquisition of products and/or services, should include an assessment capable of identifying potential cyber security risks.

- SA-3 Lifecycle Support: All <Organization Name> project/program lifecycle methodologies should be cross referenced with security lifecycle activities as described by the Office of Information Security.
- SA-4 Security Configuration: All <Organization Name> businesses procuring technology for use in any <Organization Name> computing environment should be provided documentation which states the security configurations of the technology, maintenance processes/procedures required for normal operation and release of known vulnerabilities associated with the technology being acquired.
- SA-5 Use Restrictions: All <Organization Name> use of procured products and services must be done in compliance with applicable vendor copyright laws, use restrictions and any other elements which may violate rules or laws under which products or services are protected.
- SA-6 Supply Chain: All vendors supplying products and/or services are required to provide <Organization Name> with information indicating the chain of supply from which the product and/or service came, including:
    - Product/service origin.
    - Product/service delivery methodology (e.g., any foreign countries that have handled the product or are responsible for the service).
    - Product/service support origin.
    - Documentation confirming the vendor's personnel have each met the terms and conditions of <Organization Name> pre-employment personnel assessment processes and procedures.
- SA-7 Confidentiality: All vendors supplying products and/or services are required to keep confidential any security related information provided to them in regards to <Organization Name> security posture, including information about <Organization Name> enterprise architecture, <Organization Name> security processes and procedures, <Organization Name> security policies, and any other information deemed by <Organization Name> that could potentially have an impact on <Organization Name> security posture. Vendors should sign a confidentiality statement for any engagement that requires the use of non-<Organization Name> employees or staff in order to ensure that no sensitive <Organization Name> information is released to unauthorized parties.
- SA-8 Vendor Service Requirements: All vendors wishing to provide <Organization Name> with services are required to maintain a Statement of Auditing Standards (SAS) No. 70, which demonstrates compliance with internal control practices consistent with the Auditing Standards Board of the American Institute of Certified Public Accountants as codified in AU 324. <Organization Name> requires the latest SAS 70 audit report from any vendor that has been procured to provide services to <Organization Name>,

specifically for IT related support and services. In addition, service vendors, that store, manage, and/or process sensitive data, are required to complete the questionnaire located in Appendix B of this policy.

- SA-9 Access Control: All IT related products, including Applications, Databases, Network and System operating platforms must include a mechanism that can perform Access Control. Product vendors, that store, manage, and/or process sensitive data, are required to complete the questionnaire located in Appendix C of this policy.
- SA-10 Audit Logging Controls: All IT related products, including Applications, Databases, Network and System operating platforms must include a mechanism that can perform audit logging. Product vendors, that store, manage, and/or process sensitive data, are required to complete the questionnaire located in Appendix C of this policy.
- SA-11 Identifier Management: All IT related products, including Applications, Databases, Network and System operating platforms must include a mechanism that can perform identifier management. Product vendors, that store, manage, and/or process sensitive data, are required to complete the questionnaire located in Appendix C of this policy.
- SA-12 Authenticator Management: All IT related products, including Applications, Databases, Network and System operating platforms must include a mechanism that can perform authenticator management. Product vendors, that store, manage, and/or process sensitive data, are required to complete the questionnaire located in Appendix C of this policy.
- SA-13 Communications Protection: All IT related products, including Applications, Databases, Network and System operating platforms must include a mechanism that can perform communications protection. Product vendors, that store, manage, and/or process sensitive data, are required to complete the questionnaire located in Appendix C of this policy.
- SA-14 Integrity Protection: All IT related products, including Applications, Databases, Network and System operating platforms must include a mechanism that can perform integrity protection. Product vendors, that store, manage, and/or process sensitive data, are required to complete the questionnaire located in Appendix C of this policy.

## Appendix A – References

The following references illustrate public laws which have been issued on the subject of information security and should be used to demonstrate <Organization Name> responsibilities associated with protection of its information assets.

a. United States Department of Commerce National Institute for Standards and Technology (NIST) Special Publication 800-53 Recommended Security Controls for Federal Information Systems Revision 3, August 2009.

b. United States Department of Commerce National Institute of Standards and Technology Special Publication 800-23 guidelines to Federal Organizations on Security Assurance and Acquisition/ Use of Tested/Evaluated products. Recommendations of the National Institute of Standards and Technology August 1999.

## Appendix B – Services Acquisition Questionnaire

| ID | Vendor Services Questionnaire | Response | Comments (e.g., N/A) | Standard |
|---|---|---|---|---|
| S.1 | Do you have a procedure for restricting employees from accessing our information? (Can only authorized personnel on your staff access information and/or resources which are owned by <Organization Name>, and can you demonstrate how you control such access)? | | | NIST SP 800-53 Access Control |
| S.2 | Do you provide security training and awareness to members of your staff who will have access to <Organization Name> information and resources?  (Can you provide <Organization Name> with the content that you use to train members of your staff)? | | | NIST SP 800-53 Awareness and Training |
| S.3 | Do you log and record transactions initiated by members of your staff who have access to <Organization Name> information and operated resources (Can you provide us with a sample of logs which show user transactions)? | | | NIST SP 800-53 Audit and Accountability |
| S.4 | Do you maintain secure baseline security configurations on your computer information systems which house <Organization Name> data (for example do you configure your systems in accordance with NIST FDCC standards or DISA Security Technical Implementation Guidelines)? | | | NIST SP 800-53 Configuration Management |

| ID | Vendor Services Questionnaire | Response | Comments (e.g., N/A) | Standard |
|---|---|---|---|---|
| S.5 | Do you pay a third party to at least annually conduct a security assessment of your computing environment, including penetration testing and an evaluation of your security policies, processes and procedures (Can you provide <Organization Name> with evidence that demonstrates that such an assessment was accomplished including the results)? | | | NIST SP 800-53 Security Assessment and Authorization |
| S.6 | Do you maintain a contingency plan which outlines how you will backup and restore <Organization Name> data that you might hold on site (Can you provide <Organization Name> with a copy of your contingency plan)? | | | NIST SP 800-53 Contingency Planning |
| S.7 | Do you require all members of your staff who will have access to <Organization Name> information and resources to have unique identifiers and to use authentication practices that meet best practices and standards (For example do all users have unique user IDs and are all user passwords required to be at least 8 characters in length, require a mix of uppercase, lowercase, special character, and numbers and can you provide us with a sample list of users and their associated user IDs matched to their names, in addition to your internal password policy as a screenshot from your domain, workstation or server policy)? | | | NIST SP 800-53 Identification and Authentication |

| ID | Vendor Services Questionnaire | Response | Comments (e.g., N/A) | Standard |
|---|---|---|---|---|
| S.8 | Do you maintain a process that is documented, including workflows which illustrate how you identify cyber security incidents, how you notify affected parties of incidents, procedures to contain identified incidents, eradication strategies for incidents and how you would recover from incidents (Can you provide <Organization Name> with an example of how you have tested and executed your incident response plan)? | | | NIST SP 800-53 Incident Response |
| S.9 | Do you allow third parties (for example vendors, consultants, etc) external to your organization to access <Organization Name> information and resources; including systems containing our data at your facility (Can you tell us what your security processes are for managing maintenance personnel access)? | | | NIST SP 800-53 Maintenance |
| S.10 | Do you store <Organization Name> data on any media and if you do, is the media non-portable (for example; <Organization Name> data is not stored on CDROMs, USB Drives, etc) and is <Organization Name> data encrypted in storage (Can you provide us with a description of how you will store our data and evidence which demonstrates that it will never be moved to mobile media)? | | | NIST SP 800-53 Media Protection |

| ID | Vendor Services Questionnaire | Response | Comments (e.g., N/A) | Standard |
|---|---|---|---|---|
| S.11 | Do you pay a third party to at least annually conduct a physical and environmental security assessment of your computing environment (i.e. data center) including where members of your staff will access <Organization Name> information and resources (Can you provide us with the results of any physical security assessments which have been conducted)? | | | NIST SP 800-53 Physical and Environmental Protection |
| S.12 | Do you maintain a Security Program Plan which documents how you manage security within your environment (Can you provide us with a copy of your security program plan)? | | | NIST SP 800-53 Planning |
| S.13 | Do you require all members of your staff with access to <Organization Name> information and resources to undergo a background investigation which includes verification of their social security numbers, as well as a criminal history check, and do you have adjudication procedures which are used to deny or accept employment based on the results of the criminal history check and social security number verification (Can you provide us with a copy of your adjudication criteria)? | | | NIST SP 800-53 Personnel Security |
| S.14 | Do you conduct internal risk assessments of the systems that you will be using to house <Organization Name> information and resources? (Can you provide us with your risk assessment methodology as well as the results of any assessments conducted for assets you own which you plan to use to connect to our resources)? | | | NIST SP 800-53 Risk Assessment |

| **<Organization Name>** | **Information Security System and Services Acquisition Policy** | |
|---|---|---|
| Department Name | Policy # | **Issue Date:**<br>September 13, 2013 |
| Approved by: | | |

| ID | Vendor Services Questionnaire | Response | Comments (e.g., N/A) | Standard |
|---|---|---|---|---|
| S.15 | Do the systems and resources that you use to store <Organization Name> information and resources meet the requirements which have been identified in sections; SA-9, SA-10, SA-11, SA-12, and SA-13 of the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53? (Can you demonstrate that you have assessed the systems that you plan on using for accessing <Organization Name> owned and operated resources)? | | | NIST SP 800-53 System and Services Acquisition |
| S.16 | Do you ensure that communications between your site and <Organization Name> maintain proper communications protections which would prevent; eavesdropping, man in the middle attacks or any other attack which could be used to access <Organization Name> data (Can you provide us with an illustration on how you protect communications between each site, for example an diagram of how your sites VPN solution is set up or a network topology diagram)? | | | NIST SP 800-53 System Communications Protection |
| S.17 | Do you maintain integrity protections on systems that you will use to access <Organization Name> information and resources (For example do you maintain anti-virus and patch management on all systems that you will use to access <Organization Name> information and resources and can you tell us specifically which Antivirus programs you use to accomplish this as well as your process for patching)? | | | NIST SP 800-53 System and Information Integrity |

## Appendix C – Products Acquisition Questionnaire

| ID | Vendor Product Questionnaire | Response | Comments (e.g., N/A) | Policy/Standard Reference |
|---|---|---|---|---|
| P.1 | Does the product support the creation of unique user identifiers and associated authentication features that can be integrated using lightweight access directory protocol and secure lightweight directory access protocol? | | | NIST SP 800-53 Access Control |
| P.2 | Does the product allow configuration of access control groups for unique user identifiers? | | | NIST SP 800-53 Access Control |
| P.3 | Is the product capable of demonstrating approval of unique user identifiers by an authorizing party (e.g., super user/administrator)? | | | NIST SP 800-53 Access Control |
| P.4 | Does the product support access restrictions based on group assignments including unique identifiers or groups which can read, write and execute files, commands or code associated with commands? | | | NIST SP 800-53 Access Control |
| P.5 | Does the product allow unique user identifiers to be activated, deactivated, and/or deleted? | | | NIST SP 800-53 Access Control |
| P.6 | Does the product support the ability to automatically disable access based on a preset period of time established by <Organization Name>? | | | NIST SP 800-53 Access Control |
| P.7 | Does the product support audit logging and email notification in the event of account creation, | | | NIST SP 800-53 Access Control |

| ID | Vendor Product Questionnaire | Response | Comments (e.g., N/A) | Policy/Standard Reference |
|---|---|---|---|---|
| | modification, disabling and termination actions? | | | |
| P.8 | Does the product support automatic logout in the event of inactivity from unique user identifiers? | | | NIST SP 800-53 Access Control |
| P.9 | Does the product allow monitoring and reporting (e.g., email) of system account usage? | | | NIST SP 800-53 Access Control |
| P.10 | Does the product support automated alerts in the event that a unique user identifier or system account is used outside of a preset period of time as determined by <Organization Name>. | | | NIST SP 800-53 Access Control |
| P.11 | Does the product allow reporting on atypical usage of unique user identifier or system accounts via electronic mail. | | | NIST SP 800-53 Access Control |
| P.12 | Does the product support reporting on user privileges via electronic mail? | | | NIST SP 800-53 Access Control |
| P.13 | Is the product capable of tracking and monitoring the assignment of privileged roles (privileged roles are defined as unique user identifiers or system accounts with read, write and execute permissions) via electronic mail? | | | NIST SP 800-53 Access Control |
| P.14 | Does the product support the ability to restrict access to it by Internet Protocol Address? | | | NIST SP 800-53 Access Control |
| P.15 | Does the product support assignment of discretionary or mandatory access control? | | | NIST SP 800-53 Access Control |

| ID | Vendor Product Questionnaire | Response | Comments (e.g., N/A) | Policy/Standard Reference |
|---|---|---|---|---|
| P.16 | Does the product support the ability to restrict information flow control on metadata? | | | NIST SP 800-53 Access Control |
| P.17 | Is the product capable preventing encrypted data from bypassing content-checking mechanisms? | | | NIST SP 800-53 Access Control |
| P.18 | Does the product allow configuration of unique user identifiers and system accounts with different access permissions separating key functions based on user or group (i.e., separation of duties). | | | NIST SP 800-53 Access Control |
| P.19 | Is the product capable of restricting access based on role or group (e.g., group account policy)? | | | NIST SP 800-53 Access Control |
| P.20 | Is the product capable of logging unsuccessful logon attempts and automatically disabling unique user identifiers or system accounts based on a present number of unsuccessful attempts as defined by <Organization Name>? | | | NIST SP 800-53 Access Control |
| P.21 | Does the product support configuration of a logon banner prior to permitting access that has content defined by <Organization Name>? | | | NIST SP 800-53 Access Control |
| P.22 | Does the product support logging of last successful and unsuccessful logon attempt for unique identifiers? | | | NIST SP 800-53 Access Control |
| P.23 | Is the product capable of restricting the number of sessions that are allowed to itself as defined by | | | NIST SP 800-53 Access Control |

| ID | Vendor Product Questionnaire | Response | Comments (e.g., N/A) | Policy/Standard Reference |
|---|---|---|---|---|
| | <Organization Name>? | | | |
| P.24 | Is the product capable of locking a session automatically after a preset period of time as defined by <Organization Name>? | | | NIST SP 800-53 Access Control |
| P.25 | Is the product capable of requiring all transactions have an associated unique user identifier or system account prior to transaction initiation? | | | NIST SP 800-53 Access Control |
| P.26 | Is the product capable of tagging information with access permission rights, so that the information can only be viewed with proper credentials regardless of where it is stored? | | | NIST SP 800-53 Access Control |
| P.27 | Is the product capable of restricting remote access except through approved <Organization Name> mediums such as the Virtual Private Networking (VPN) infrastructure? | | | NIST SP 800-53 Access Control |
| P.28 | Is the product capable of restricting wireless access except through approved <Organization Name> wireless solutions? (See <Organization Name> Information Security Policy on Wireless). | | | NIST SP 800-53 Access Control |
| P.29 | Is the product capable restricting unique user identifiers' access to other unique user identifiers' information, directory structure, etc. unless otherwise permitted by a user with super | | | NIST SP 800-53 Access Control |

| ID | Vendor Product Questionnaire | Response | Comments (e.g., N/A) | Policy/Standard Reference |
|---|---|---|---|---|
| | user/administrative access? | | | |
| P.30 | Is the product capable of logging and recording all unique user identifier activity and system account activity? | | | NIST SP 800-53 Audit and Accountability |
| P.31 | Is the product capable of logging and recording all changes which occur on the asset including applications, databases, network or system operating systems? | | | NIST SP 800-53 Audit and Accountability |
| P.32 | Is the product capable of logging system and activity transactions including date, time and whether the event was successful? | | | NIST SP 800-53 Audit and Accountability |
| P.33 | Is the product capable of storing log data on a predefined amount of storage as defined by <Organization Name>? | | | NIST SP 800-53 Audit and Accountability |
| P.34 | Is the product capable of alerting via email if log data is not successfully recorded? | | | NIST SP 800-53 Audit and Accountability |
| P.35 | Is the product capable of recording software / hardware errors and when storage capacity has been reached? | | | NIST SP 800-53 Audit and Accountability |
| P.36 | Is the product capable of logging messages using the "syslog" or "syslog-ng" protocol in compliance with RFC 3164? | | | NIST SP 800-53 Audit and Accountability |
| P.37 | Does the product support filtering capabilities for all specified log types that are captured by the asset (e.g., application, database, network | | | NIST SP 800-53 Audit and Accountability |

| ID | Vendor Product Questionnaire | Response | Comments (e.g., N/A) | Policy/Standard Reference |
|---|---|---|---|---|
| | or system operating systems)? | | | |
| P.38 | Does the product support time stamps of transactions and events for purposes of logging? | | | NIST SP 800-53 Audit and Accountability |
| P.39 | Does the product support data storage using encryption algorithms that exceed the strength of 128-bit advanced encryption standard? | | | NIST SP 800-53 Audit and Accountability |
| P.40 | Does the product support utilization of hashing and/or generally accepted digital signature based technology to provide non-repudiation of logs stored or transmitted from the asset including applications, database, network or system operating systems? | | | NIST SP 800-53 Audit and Accountability |
| P.41 | Does the product support the retention of log data for a preset period of time (in storage) as defined by <Organization Name>? | | | NIST SP 800-53 Audit and Accountability |
| P.42 | Does the product require unique user identification before access is granted to an asset including applications, databases, network or system operating platforms? | | | NIST SP 800-53 Identification and Authorization |
| P.43 | Does the product require unique system identification before system-to-system access is allowed? | | | NIST SP 800-53 Identification and Authorization |
| P.44 | Is the product capable of establishing user accounts based on unique attributes such as last names, initials, etc. at the | | | NIST SP 800-53 Identification and Authorization |

| ID | Vendor Product Questionnaire | Response | Comments (e.g., N/A) | Policy/Standard Reference |
|---|---|---|---|---|
| | discretion of <Organization Name>? | | | |
| P.45 | Is the product capable of restricting the permanent use of a unique user identifier that has already been used? | | | NIST SP 800-53 Identification and Authorization |
| P.46 | Does the product require the authentication of a unique user identifier prior to permitting access to the requested resource? | | | NIST SP 800-53 Identification and Authorization |
| P.47 | Is the product capable of supporting password strings of at least 15 characters during password authentication? | | | NIST SP 800-53 Identification and Authorization |
| P.48 | Is the product capable of enforcing password complexity which requires the use of at least 1 uppercase, 1 lowercase, 1 special character, and 1 number? | | | NIST SP 800-53 Identification and Authorization |
| P.49 | Is the product capable of enforcing that new passwords for unique user identifiers cannot use previous password sequences where at least 6 characters are being reused? | | | NIST SP 800-53 Identification and Authorization |
| P.50 | Does the product support password storage using at least 128-bit advanced encryption standard? | | | NIST SP 800-53 Identification and Authorization |
| P.51 | Is the product capable of expiring passwords and requiring unique user identifiers to change their password after a preset period of time not to exceed 365 days and at the discretion of <Organization | | | NIST SP 800-53 Identification and Authorization |

| ID | Vendor Product Questionnaire | Response | Comments (e.g., N/A) | Policy/Standard Reference |
|---|---|---|---|---|
| | Name>? | | | |
| P.52 | Does the product support the use of PKI-based authentication solutions? | | | NIST SP 800-53 Identification and Authorization |
| P.53 | Does the product support the use of PKI including validation of certificates through the construction of certification paths with status information to an accepted trust anchor? | | | NIST SP 800-53 Identification and Authorization |
| P.54 | Does the product support the use of PKI including enforcement of authorized access to the corresponding private keys? | | | NIST SP 800-53 Identification and Authorization |
| P.55 | Does the product support the use of PKI maps authenticated identities to unique user identifiers? | | | NIST SP 800-53 Identification and Authorization |
| P.56 | Is the product capable of masking passwords during system entry? (i.e., shows passwords as ******). | | | NIST SP 800-53 Identification and Authorization |
| P.57 | Does the product support cryptographic authentication schemes which are at a minimum in compliance with FIPS 140-2 (i.e. 128-bit AES for example is acceptable)? | | | NIST SP 800-53 Identification and Authorization |
| P.58 | Is the product capable of separating the administration of the asset from the use of the asset (i.e., Application Partitioning) including applications, databases, network or system operating platforms? | | | NIST SP 800-53 System and Communications Protection |

| ID | Vendor Product Questionnaire | Response | Comments (e.g., N/A) | Policy/Standard Reference |
|---|---|---|---|---|
| P.59 | Is the product capable of requiring unique user identification and authentication to shared resources, and all activity and use of the resource is logged, recorded and reported? | | | NIST SP 800-53 System and Communications Protection |
| P.60 | Is the product capable of restricting access from specific sources using specific protocols? | | | NIST SP 800-53 System and Communications Protection |
| P.61 | Is the product capable of prioritizing services as determined by <Organization Name> to enhance performance (generally only applied to operating platforms)? | | | NIST SP 800-53 System and Communications Protection |
| P.62 | Is this product capable of preventing access via Internet Protocol, Service and Port? | | | NIST SP 800-53 System and Communications Protection |
| P.63 | Does this product support checksums and hash values to maintain the integrity of information? | | | NIST SP 800-53 System and Communications Protection |
| P.64 | Is this product capable of encrypting data in transit to protect it from unauthorized disclosure? | | | NIST SP 800-53 System and Communications Protection |
| P.65 | Is this product capable of terminating communications when sessions are completed? | | | NIST SP 800-53 System and Communications Protection |
| P.66 | Can the product be configured to communicate only with specific assets? | | | NIST SP 800-53 System and Communications Protection |
| P.67 | Is the product capable of utilizing PKI infrastructures? | | | NIST SP 800-53 System and |

| ID | Vendor Product Questionnaire | Response | Comments (e.g., N/A) | Policy/Standard Reference |
|---|---|---|---|---|
|  |  |  |  | Communications Protection |
| P.68 | Is the product capable of utilizing only FIPS 140-2 compliant encryption algorithms (e.g., 128-bit AES)? |  |  | NIST SP 800-53 System and Communications Protection |
| P.69 | Does the product support the ability to use acceptable mobile code such as Java, JavaScript, ActiveX, PDF, Postscript, Shockwave movies, Flash animations, and VBScript? |  |  | NIST SP 800-53 System and Communications Protection |
| P.70 | Does the product support session authenticity during initialization of sessions (e.g., SSL)? |  |  | NIST SP 800-53 System and Communications Protection |
| P.71 | Does the product support the ability to have vendor’s correct flaws (e.g., security vulnerabilities) including applications, databases, network and system operating platforms? |  |  | NIST SP 800-53 System and Information Integrity |
| P.72 | Is the product capable of being scanned using well-known antivirus systems for malicious code? |  |  | NIST SP 800-53 System and Information Integrity |
| P.73 | Is the product capable of restricting personnel from entering data in the asset based on access control (e.g., role-based access)? |  |  | NIST SP 800-53 System and Information Integrity |
| P.74 | Does the product have the ability to determine whether or not inputs are valid? |  |  | NIST SP 800-53 System and Information Integrity |