Cloud Computing Framework

Technology Department

Updated: 6/24/2016
Version: 1.3

The Agency's Cloud Framework consists of components and/or controls that must be addressed when selecting a Public Cloud service or Software as a Service (SaaS) vendor. The elements in this framework are dynamic and will evolve over time to ensure a secure and robust Cloud Computing environment for the Agency's business.
Intentionally Left Blank
## REVISION HISTORY

<table>
<thead>
<tr>
<th>Version</th>
<th>REVISION DATE</th>
<th>REVISION DESCRIPTION</th>
<th>REVISION TRACKING NOTES</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.0</td>
<td>12/14/2015</td>
<td>Baseline Draft Version</td>
<td></td>
</tr>
<tr>
<td>1.1</td>
<td>12/17/2015</td>
<td>Reformatting Document</td>
<td>Added Document Template</td>
</tr>
<tr>
<td>1.1.1</td>
<td>12/17/2015</td>
<td>Incorporated Department Comments</td>
<td>Included new Password Policy Language</td>
</tr>
<tr>
<td>1.2</td>
<td>02/03/2016</td>
<td>Incorporated Audit Document Revised Checklist (1/26/2016)</td>
<td>Modified Cover page</td>
</tr>
<tr>
<td>1.3</td>
<td>06/24/2016</td>
<td>Modified Section 14 Password Policies and Requirements</td>
<td>Remove password syntax</td>
</tr>
</tbody>
</table>
The Agency’s Cloud Framework consists of components and/or controls that must be addressed when selecting a Public Cloud service or Software as a Service (SaaS) vendor. The elements in this framework are dynamic and will evolve over time to ensure a secure and robust Cloud Computing environment for the Agency’s business. The Framework elements consist of the following components and/or controls:

1. Cloud Offering:

2. The Agency Cloud Framework:
   The Framework is meant to ensure that all physical, logical and information assets are secure and that security and privacy are maintained using de-facto best practices aligned with Federal Information Processing Standards (FIPS) as well as NIST Publications. To that end, Cloud Solutions should be compliant with the latest versions of the following best practices (as appropriate for application risk), to name a few:
   a. NIST 800-144: Guidelines on Security and Privacy in Public Cloud Computing
   b. FIPS 199: Standards for Security Categorization of Federal Information and Information System
   c. FIPS 200: Minimum Security Requirements for Federal Information and Information Systems
   d. NIST 800-53: Recommended Security Controls for Federal Information Systems and Organizations
   e. NIST 800-146: Cloud Computing Synopsis and Recommendations
   f. Cloud Security Alliance: Cloud Controls Matrix Version 3.0 (CCMv3)

3. For Software-as-a-Service (SaaS), excerpt from NIST 800-146:
   a. Data Protection. Analyze the SaaS provider’s data protection mechanisms, data location configuration and database organization/transaction processing technologies, and assess whether they will meet the confidentiality, compliance, integrity and availability needs of the Agency.
   b. Client Device/Application Protection. Consistent with the FIPS 199 impact level of the data being processed, protect the Agency’s client device (e.g., a computer running a Web browser) so as to control the exposure to attacks.
   c. Encryption. Require that strong encryption using a robust algorithm with keys of required strength be used for Web sessions whenever the subscribed SaaS application requires the confidentiality of application interaction and data transfers. Also require that the same diligence be applied to stored data. Federal agencies must employ government-approved cryptographic algorithms for encryption and digital signature, and the implementations need to be FIPS 140-2 validated. Understand how cryptographic keys are managed and who has access to them. Ensure that cryptographic keys are adequately protected.
   d. Secure Data Deletion. Require that cloud/vendor providers offer a mechanism for reliably deleting data at the Agency’s request.

4. Data Location:

5. Electronic Discovery:
   a. A cloud/vendor’s information archival capabilities must preserve the original metadata of ‘client data’ so as to not adversely affect the Agency’s litigation risk

6. Data Ownership:
   The Agency retains exclusive ownership over all its data:
   a. That the cloud/vendor provider acquires no rights or licenses to that data, including intellectual property rights or licenses.
   b. The cloud/vendor may not use the Agency’s data for its own purposes;
   c. and that the cloud/vendor does not acquire and may not claim any interest in the data due to security.

7. Availability:
   a. Must meet 99.9% uptime

8. Physical Security:
   a. 24-hour monitoring of data centers.
   b. Multi-factor authentication, including biometric scanning for data center access.
c. Internal data center network is segregated from the external network.
d. Role separation renders location of specific customer data unintelligible to the personnel that have physical access.
e. Faulty drives and hardware are demagnetized and destroyed.

9. Logical Security:
   a. Lock box processes for strictly supervised escalation process greatly limits human access to your data.
   b. Servers run only processes on whitelisted, minimizing risk from malicious code.
   c. Dedicated threat management teams proactively anticipate, prevent, and mitigate malicious access.
   d. Port scanning, perimeter vulnerability scanning, and intrusion detection prevent or detect any malicious access.

10. Data Security:
    a. Encryption at rest protects the Agency’s data on cloud/vendor servers.
    b. Encryption in transit with SSL/TLS protects Agency’s data transmitted between the Agency and cloud/vendor application.
    c. Threat management, security monitoring, and file/data integrity prevents or detects any tampering of data.

11. Compliance Standards:
    a. **Health Insurance Portability and Accountability Act (HIPAA):** HIPAA imposes, under law, certain requirements for security, privacy, and reporting regarding the processing of electronic protected health information.
    b. **Federal Information Security Management Act (FISMA):** requires U.S. federal agencies to develop, document, and implement controls to secure their information and information systems. Federal Risk and Authorization Program (FedRAMP) is a federal risk management program that provides a standardized approach for assessing and monitoring the security of cloud products and services.
    c. **ISO 27001 Certification:** Along with NIST 800-53, ISO 27001 is one of the best security benchmarks available. Cloud/vendor should comply with the set of physical, logical, process and management controls defined by ISO 27001:2013, inclusive of ISO 27018 Privacy controls.
    d. **European Union (EU) Model Clauses:** The EU Data Protection Directive, a key instrument of EU privacy and human rights law. The EU model clauses are recognized as a preferred method for legitimizing the transfer of personal data outside the EU for cloud computing environments. Supporting the EU model clauses involves investing and building the operational controls and processes required to meet the exacting requirements of the EU model clauses. Unless a cloud/vendor service provider is willing to agree to the EU model clauses, the Agency might lack confidence that it can comply with the EU Data Protection Directive’s requirements for the transfer of personal data from the EU to jurisdictions that do not provide “adequate protection” for personal data.
    e. **U.S.–EU Safe Harbor framework:** The U.S.-EU Safe Harbor framework also enables the Agency, as needed, to legally transfer personal data outside of the EU under the EU Data Protection Directive.
    f. **Statement on Standards for Attestation Engagements No. 16 (SSAE 16):** Cloud/vendor has been audited by independent third parties and can provide SSAE16 SOC 1 Type I and Type II and SOC 2 Type II reports on how the service implements controls.
    g. **Canadian Personal Information Protection and Electronic Documents Act (PIPEDA):** The Canadian Personal Information Protection and Electronic Documents Act pertains to how private sector organizations collect, use, and disclose personal information in the course of commercial business.
    h. **Gramm–Leach–Billey Act (GLBA):** The Gramm–Leach–Billey Act requires financial institutions to put processes in place to protect their clients’ nonpublic personal information. GLBA enforces policies to protect information from foreseeable threats in security and data integrity.
12. Audit Control Requirements:

a. General:
   1. Documented procedures, flowcharts and process maps for the application.
   2. Conduct regular audits, vulnerability testing, and security scanners.
   3. SSAE 16 SOC 2 Type II (previously known as SAS 70 Level 2)
   5. ISO27001 Certification
   6. Criminal Justice Information Services (CJIS) security policies and procedures compliant for law enforcement information and systems.
   7. Background check should be performed on all personnel.

b. System/Security Administration
   1. Administrative personnel should receive training.
   2. Administrative staff should receive general security awareness training before access is provided. All security training must be reinforced at least every three years and must be tracked as per the PA Information Security Handbook.
   3. System and security administration procedures should be documented and distributed.
   4. Administrator(s) roles and responsibilities should be documented.
   5. Developers and/or programmers should not have access to the production server.
   6. Operating system administrators should not have access to the production database and application.

c. Hardening of operating system/database that supports the application:
   1. Disable and/or remove unnecessary ports/services.
   2. Remove all manufacturer samples from the production system. Scripts must be removed from production systems, except those required for the operation and maintenance of the system.
   3. Default, public, and guest accounts should be secured/locked/removed.
   4. Change all default passwords; delete all default content and login scripts.
   5. Limit administrative and user account privilege and access.
   6. Document system accounts like administrator, root, oracle, and sys.
   7. Document user/group access rights
      a. Users/groups should be setup with least access required to perform job responsibilities.
   8. Implement access control at the database level (i.e. user roles and permissions, passwords, secure links)
   9. Use secure encrypted remote access methods.
   10. If the application is a web application, log (and monitor) web traffic and trend the activity looking for abnormal activity.
   11. Ensure that appropriate security and vulnerability assessment tools are running.
   12. At login, last user login should not display.
   13. Inventory listing of hardware and software should be current and maintained.

d. License Management:
   1. Ensure that application licensing requirements are documented, reviewed and maintained.
   2. Application licenses should be current/valid and individuals/groups with application access should have completed the necessary access request forms and adhere to licensing requirements.

e. Logical Access Controls:
   1. All users are required to read the Agency Policy Computing Resource Administrative Instruction (AI 15-4.03) and sign an acknowledgement of the Agency IT Acceptable Use Code of Conduct policy prior to account activation.
   2. Procedures to grant/modify/delete access should be documented.
      a. Access request forms for adding/modifying/deleting users should be used.
      b. Account expiration for contractors and consultants.
      c. Accounts adequately identify the user – no generic accounts

---

1 Audit Department 1/26/2016 Update, with TEC Department modifications to password policies
3. Ensure that security administrator procedures exist to:
   a. Create/remove application access in a timely manner
   b. Review user roles/permissions
4. Validate that all users have accessed the application within the past 90 days.
   a. Review dormant accounts
   b. Inactive accounts should be removed.
5. Each user has a unique user ID as described in the Port Authority Standard and Guidelines.
   a. All user accounts profile should include Employee ID# and full user name.
6. Roles are setup with least access required to perform job responsibilities.
7. Roles should have a segregation of duties/roles.
8. All accounts must have an individual or business group assigned to be responsible for account management.
9. Segregation of duties and areas of responsibility must be implemented where appropriate.
10. Whenever segregation of duties is not technically feasible, other compensatory controls must be implemented, such as monitoring of activities, audit trails and management supervision. The PA must approve these compensating controls.
11. Review of audit trails and system approvals must be performed independent and retained to document the implementation of these security controls
12. Access Control List (ACL) should include:
    a. Current list of ACL
    b. Creation and updates to ACL
    c. Testing and approvals of ACL
13. The application should have the PA's warning banner on the login screen. The application has a warning banner, terms of use, and/or privacy statement that was approved by the Port Authority on the login screen.
14. The system should have an access role that would allow real only access to all application, database and operating system screens, functions, logs and reports.
15. Remote access should be approved, secured, and documented in accordance with PA policy. Remote access, at a minimum, must consist of multifactor authentication mechanisms, secured communications (TLS/VPN encryption methodology), access control mechanisms and logging of user activity.

f. Password Controls: (see Section 14. Port Authority Password Policies and Requirements)

g. Application Controls:
1. Data Validation & Input Controls
   a. The application should have input controls to verify the validity of the data entered.
2. Data Retention and Management
   a. All data should be classified according to its sensitivity (confidential, etc) and protected accordingly.
   b. Data archive strategy should be documented and in place.
      i. Should specify how long active data is kept.
4. Data Integrity and Security
   a. Sensitive data, such as credit card #s and social security #s, should be encrypted.
   b. Data should be restricted and audit trails should be available to identify all user activity include view access to sensitive data.
   c. Data should be stored in the database encrypted and blocked from user views in the application unless it is authorized.
   d. Encryptions level at a minimum should be AES 256bit when encryption is used.

5. Application Interfaces:
   a. Interface file should be secured and archived.
   b. Reconciliation of data should be done on a batch record and totals. Detail data reconciliations should be completed on periodic basis.
6. Processing Controls:
   a. Application databases/interfaces should have the necessary controls to prevent processing of inaccurate, duplicate, or unauthorized transactions and producing inaccurate outputs.
   b. Controls to ensure that all data is processed and accounted for should be in place.
   c. Rejected items should be logged, tracked and resolved in a timely manner.

h. Change Management:
1. Processes and tools should be used to report, track, approve, fix, and monitor changes on the application.
2. The application and all changes to the application should be tested before being put into production.
   a. Documentation of approval for change and evidence of testing should be in place.
   b. Specific timetable/schedule should be documented.
3. Emergency procedures should be documented and distributed.
4. Separate environments are required for development, test, quality assurance, production.
5. Procedures should require that no changes be made directly in the production environment without going through the development/test/quality assurance environments.
6. Formal change control procedures for all systems must be developed, implemented and enforced.
7. Where technically feasible, development software and tools must not be maintained on production systems.
8. Source code for application or software must not be stored on the production system running that application or software.
9. Privileged access to production systems by development staff must be restricted.

i. Application Logging, Audit Trails and Record Retention:
1. Audit trails for operating, application, and database systems should exist and reviewed.
2. Users and roles should be tracked and reviewed
   a. Maintain documentation
3. All failed logon attempts should be logged.
4. All sensitive transactions and changes should be logged and an audit trail created.
5. Audit trails should contain who made the change, when it was made, and what was changed.
6. Only the security administrator should have access to change or delete these logs or audit trails.
7. Audit trails should be reviewed by the business owner(s) and security administrator.
8. Management reporting should be produced through the application.
9. Access reports by user and privilege should be produced and reviewed periodically including access violation reports and exception transaction reporting.

j. Contingency Planning, Disaster Recovery and Backup Management:
1. A business contingency plan and a disaster recovery plan for the application should be documented and stored off-site, including escalation plan and current call tree.
2. Plans should be tested and the outcomes of the tests (success/failure) should be documented.
3. Regular backups of the application and the application data should be stored off-site.
4. Application executables should be stored off-site or in escrow.
5. Application configurations should be documented and backed-up.
6. Full system backup should be encrypted.
7. Backup procedures should be documented.
8. Tape maintenance should include:
   a. Periodically testing integrity of tape
   b. Procedures for tape destruction due to faulty or scratched hardware.

k. Performance Monitoring:
1. Incident monitoring procedures should be documented and incidents logs should be reviewed to ensure that appropriate action is taken.
2. Performance statistics should be examined and reviewed periodically by system administrators/business owner(s).
3. If vendor(s) support the application, a service level agreement for uptime, performance monitoring, updates, etc should be confirmed.
4. Baseline tools or security products should be used and checked on a quarterly basis.

I. Patch Management:
1. Patch management procedures and documentation
   a. Procedures should include testing, approvals, and distribution.
   b. Documentation should include emergency procedures.
2. Apply all new patches and fixes to operating system and application software for security.
3. All security patches must be reviewed, evaluated and appropriately applied in a timely manner. This process must be automated, where technically possible.

m. Physical Protection:
1. Physical access to the application hardware should be appropriately restricted.
   a. Physical access secured by single authentication mechanism i.e. swipe card.
   b. Physical security adequate for equipment (locked cabinets)
2. Appropriate fire suppression systems should be in place.
3. Environmental condition adequately controlled (no water, dirt, clutter) and monitored.
   a. Temperature and humidity monitoring should be implemented.
4. Security cameras installed in sensitive areas
5. Power surge protection and emergency power backup are in place.
6. All hardware and software assets must be inventoryed.
7. Visitors including maintenance personnel, to data center, server and network equipment storage facilities must be escorted at all times.

n. Anti-virus Management / Integrity / Vulnerability Software Management:
1. Virus patch management procedures must be documented, including emergency update procedures.
2. Anti-virus and software integrity checkers must be implemented to prevent and detect the introduction of malicious code or other threats.
3. Virus software engines and definitions must be implemented and up-to-date.
4. A remote distribution server should be implemented for virus software updates and documentation on remote distribution should be current and maintained.
5. Intrusion detection system must be in place,
6. All systems must have vulnerability scans performed before going into production and periodically thereafter. Appropriate action, such as patching or updating the system, must be taken to address discovered vulnerabilities.
7. Host-based intrusion detection/ firewalls software must be installed and enabled on all systems to protect from threats and to restrict access. Incident response procedures must be in place to address any alerts identified and system owner should be notified of alerts and what action was taken to mitigate the issues.
8. Monitoring systems must be deployed (e.g., intrusion detection/prevention systems) at strategic network locations to monitor inbound, outbound and internal network traffic.
9. Monitoring systems must be configured to alert incident response personnel to indications of compromise or potential compromise.
10. Procedures must be established to maintain information security during an adverse event.
11. Firewalls should be implemented.
12. Firewall rules documentation should be up-to-date.
13. Network management connections must be performed from a secure, dedicated network.

o. Wireless Device:
1. Devices should be using WPA/WPA2 and AES encryption or better.
2. Devices should disallow broadcasting of the SSID.
3. All default parameters should be changed.
4. Devices should have MAC address filtering enabled or some type of authentication mechanism in place.
p. Web Application Vulnerabilities and Controls:
1. Best Practice and Standards:
   a. The Open Web Application Security Project (OWASP) - [www.owasp.org](http://www.owasp.org)
   b. [www.webappsec.org](http://www.webappsec.org) (a consortium of web application security professionals)
   c. Center for Internet Security (CIS) – [www.cisecurity.org](http://www.cisecurity.org)
2. Perform data validation & integrity checks for field values and ensure the HTML special characters are strippper for all HTML request.
3. Do not allow site pages to be cached by user browsers.
4. All sensitive, personal or confidential data (including SSN, passwords, session IDs for sensitive applications, confidential or sensitive business transactions, etc.) should be transmitted between browser and server within an SSL-encrypted session (or other encrypted transmission) and are encrypted in the database at rest.
5. All sensitive and personal data should be masked and encrypted were possible.
6. Legal Issues:
   a. The site should have a privacy statement and term of usage.
   b. American Disability Act – Section 508 should be considered during the development process due to the requirement that federal agencies’ electronic and information technology is accessible to people with disabilities.
7. Web Authentication: To prevent passwords from being passed in the clear, have authentication occur within an TLS encrypted tunnel. Use TLS (certificate) to protect the password.
8. Password Reset:
   a. For internal applications, reset passwords via the helpdesk or security administrator of the site
   b. For external applications, send temporary password to known e-mail address, that must be changed upon login and/or
   c. Have customer service reset after the user has been validated.
   d. If possible, use two factor authentication like Secure ID fobs.

q. Credit Card Processing Checklist:
1. If credit cards are accepted, PCI Standards (PCI DSS v3.1) should be followed and the process should be PCI compliant. Ensure all vendors and consultants are required to be PCI compliant. Attachment - The payment card application should be PCI compliant (PA-DSS v3.1).
2. A segregated network and/or an approved Point of Sale terminal should be in place for the system or terminal used to process credit card transactions.
3. The credit card processor standard and requirements should be followed, i.e. maintain transaction data for two years.
4. Maintain the security of the customer information, including not storing credit numbers, the cardholder CVC/CVV numbers or any of the data from the magnetic strip on the credit card.
5. Maintain the transaction data for contesting chargebacks, ensure that the processor fees are appropriate and do reconciliations of the transactions processed and the money deposited in the Port Authority bank accounts.
6. The appropriate Port Authority functional areas should be made aware credit card processing activity and should be involved applying for the Merchant ID for MasterCard/Visa, Discover and American Express.
7. Create a privacy policy and procedure for staff and consultants.
8. Perform quarterly vulnerability scans of the network that contains the credit card processing, annual PCI reviews according to the PCI DSS, and annual system penetration testing.
9. Perform the appropriate annual assessment and provide a report on compliance (ROC) which state shows compliance.

r. Credit Card Processing Checklist:
1. The Disaster Recovery plan should include at a minimum the following areas.
   a. Business Impact Analysis
   b. Critical Time Frame
   c. Application System Impact Statements
   d. Recovery Strategy & Approach
e. Recovery Time Objectives (RTO)/Recovery Point Objectives (RPO) for all critical systems.

f. Disaster Definition

g. Detailed Recovery Steps for each Disaster Definition

h. Escalation Plans and Decision Points

i. System Components- An inventory of the criticality of systems (including but not limited to software and operating systems, firewalls, switches, routers and other communication equipment).

j. Disaster Recovery Emergency Procedures

k. Plan Procedure Checklist

l. Disaster Recovery Team Organization
   i. Salvage Team & Team Responsibilities
   ii. Disaster Recovery Responsibilities
   iii. Essential Position – Require back-up personnel to be assigned.

m. Contacts information Disaster Recovery Team and critical vendors - this area should be reviewed semi-annually for updates and changes.

n. Post-Disaster – Detail what steps need to be taken to move from disaster mode back to normal operations.

2. Contingency plans (e.g., business continuity plans, disaster recovery plans, and continuity of operations plans) must be established and tested regularly.

3. Backup copies of procedures, software, and system images should be taken regularly and moved offsite.

4. Backups and restoration must be tested regularly.

13. Criminal Justice Information Services (CJIS) Compliance (as appropriate).

14. Port Authority (PA) Password Policies and Requirements:

   These requirements applies to all PA information technology systems regardless of whether they are administered by (or on behalf of) the PA.

   1. End user accounts will be disabled (not deleted) after 60 days of non-use;
   2. All information technology system account passwords will be complex. The syntax for this complex password will be published after the appropriate PANYNJ Non-Disclosure Agreement (NDA) is executed.
   3. User passwords will require a change every 90 days.
   4. All accounts will be granted the minimum level of access and permissions necessary to perform an assignment.
   5. If a system account fails to satisfy the requirements of this policy, an administrator may place the account in “disabled” status until remedied.
   6. Changes to an account’s access privileges require the appropriate managers to request new or modified access.
   7. All users are required to read the Agency Computing Resource Administrative Instruction and sign an acknowledgement of the Agency IT Acceptable Use Code of Conduct policy prior to account activation.
   8. Annually, all managers are required to certify that only authorized employees have accounts on Agency systems. Technology and the Office of the CSO will work with managers to provide them with the lists of employees and their accounts.
   9. Passwords must not be shared.
   10. Accounts should be locked after a three logon failures.
   11. Passwords should not be the same account name.
   12. No concurrent login capabilities.
   13. Password file should be securely stored with limited access and encrypted.
   14. Application forces initial passwords to be changed and the initial passwords should not be easily guessable.
   15. Set “automatic session timeout” to 15 minutes of inactivity and require user to log back in with valid ID and password.
Purpose of the following items:
   (1) so we don’t create ‘islands’ of users without a centralize mechanism to manage accounts and
   (2) protecting our *information* assets, regardless of where it may reside (in cloud, on premises, etc.)

15. Integration with the Agency’s Active Directory platform for centralized account/application user management
16. Integration with the Agency’s Information Rights Management Framework which will leverage Microsoft Azure Rights Management Services