Information Security Policy
Cloud

PURPOSE

Cloud computing offers a number of advantages including low costs, high performance and quick delivery of services. However, without adequate controls, it also exposes individuals and organizations to online threats such as data loss or theft, unauthorized access to corporate networks, and so on.

The purpose of this policy is to ensure that any introductions or changes to the [redacted] New York City - ("The Agency" or "TRSNYC") Cloud Services environments are managed and controlled through an established process utilizing best practices. This is necessary to protect the integrity and confidentiality of Agency data and the security of the Agencies network.

The Agencies IT department remains committed to enabling employees to do their jobs as efficiently as possible through the use of technology. The following guidelines are intended to establish a process whereby the Agency can use and leverage cloud services without jeopardizing Agency data and computing resources.

SCOPE

The scope of this policy pertains to:

SaaS – ***Software as a Service*** is a software licensing and delivery model in which software is licensed on a subscription basis and is centrally hosted. It is sometimes referred to as "on-demand software". SaaS is typically accessed by users using a thin client via a web browser.

IaaS –***Infrastructure as a Service*** is the most basic cloud-service model. Providers of IaaS offer computers – physical or (more often) virtual machines – and other resources. (A hypervisor, such as Xen, Oracle VirtualBox, KVM, VMware ESX/ESXi, or Hyper-V runs the virtual machines as guests. Pools of hypervisors within the cloud operational support-system can support large numbers of virtual machines and the ability to scale services up and down according to customers' varying requirements.) IaaS clouds often offer additional resources such as a virtual-machine disk image library, raw block storage, and file or object storage, firewalls, load balancers, IP addresses, virtual local area networks (VLANs), and software bundles. IaaS-cloud providers supply these resources on-demand from their large pools installed in data centers. For wide-area connectivity, customers can use either the Internet or carrier clouds (dedicated virtual private networks).

PaaS – ***Platform as a Service*** providers deliver a computing platform, typically including operating system, programming language execution environment, database, and web server. Application developers can develop and run their software solutions on a cloud platform without the cost and complexity of buying and managing the underlying hardware and software layers. With some PaaS offers like Microsoft Azure and Google App Engine, the underlying computer and storage resources scale automatically to match application demand so that the cloud user does not have to allocate resources manually. The latter has also been proposed by an architecture aiming to facilitate real-time in cloud environments. Even more specific application types can be provided via PaaS, e.g., such as media encoding as provided by services as bitcodin transcoding cloud or media.io.

POLICY

Cloud computing services are application and infrastructure resources that users access via the Internet. These services are contractually provided by third party companies enabling customers to leverage powerful computing resources that would otherwise be beyond their means to purchase and support. Cloud services provide services, platforms, and infrastructure to support a wide range of business activities. These services support, among other things, communication; collaboration; project management; scheduling; and data analysis, processing, sharing, and storage. Cloud computing services are generally easy for people and organizations to use, as they are accessible over the Internet through a variety of platforms (workstations, laptops, tablets, and smart phones), and they may be able to accommodate spikes in demand much more readily and efficiently than in-house computing services.

A. SAAS – [SOFTWARE AS A SERVICE] & PAAS – [PLATFORM AS A SERVICE]

1. A data classification template must be completed fully by the Project Manager prior to selection of the software.
2. Authentication to any SaaS or PaaS cloud service provider must be through an agency approved authentication mechanism such as ADFS, LDAP or Entrust authentication platforms where technologically feasible.
3. Authentication to SaaS or PaaS cloud services must be implemented with Single Sign On – SSO when possible.
4. Authentication must include two factor authentication mechanisms.
5. For solutions that do not leverage an Agency approved Authentication system in #2 above, the following must be identified.
   - **a.** Enabling and disabling users access to the platform
   - **b.** Active directory synchronization
   - **c.** Controls surrounding the prevention of theft of users credentials
   - **d.** Password strength
   - **e.** Monitoring users access
   - **f.** Phishing
6. Review of a SaaS or PaaS cloud solution requires a risk approval and the creation of a risk register followed by a high level sign off of the risk if the solution is deemed acceptable.
7. Implementation of SaaS or PaaS solutions must restrict the connecting routed endpoints to a single ip address.
8. The use of any Agency data rated as *Highly Confidential* is not permitted to reside on <u>any</u> cloud service. Exceptions to this may be approved in advance by the office of the Executive Director and the Chief Risk Officer.
9. Availability and capacity requirements concerning the Agency's internet connection must be taken into consideration prior to purchasing any SaaS or PaaS cloud solution.
10. Connections to any SaaS or PaaS cloud solutions will employ real time IDS, IPS, and Virus/Spyware/Malware detection employing defense in depth mechanisms.
11. All SaaS and PaaS cloud solutions must be vetted through the Agency's Security Accreditation process.
12. If the solution will use production data classified as *Highly Confidential*, then "N" tier encryption must be employed throughout the solution employing the *highest level of encryption possible*. This would include encryption at a minimum as follows:
    - **a.** Encryption from the Client PC to the Web Server.
    - **b.** Encryption from the Web Server to the Application Server.
    - **c.** Encryption from the Application Server to the Database.
    - **d.** It is recommended that the use of stored procedures also be encrypted where used.
    - **e.** Production and backup databases utilized in a solution must enable column level encryption for highly confidential data in addition to encrypting data at rest utilizing Transparent Data Encryption or equivalent technologies.
13. All Primary and Backup Co-Located Data Centers must be secure and reside within the continental US.
14. The service provider must provide an operational SSAE-16 audited control document for Agency review which would include patch management and incident response along with an SLA for availability.

15. All back end services utilized by the service provider must be secured and audited on an annual basis. This includes instances whereby the vendor has an open connection to other service provider(s) to provide the cloud based solution.
16. For testing of production solutions, all data must be fully obfuscated or masked as appropriate.
17. SAAS and PaaS solutions must employ private cloud methodologies with single tenancy either on one physical drive, or on one logical drive utilizing virtualization with firewalls.
18. Mechanisms such as Data Loss Prevention (DLP) must control file sharing/uploading/downloading of production data.
19. A plan for degaussing or deleting data must be planned for prior to engaging in a vendor contract. A certificate of data destruction must be furnished to the agency for any and all data stores used in the solution upon termination of the contract.
20. An exit plan strategy to move data to a new vendor provider should be built into the solution.
21. The cloud provider must provide a living will if one exists.
22. Connections to all cloud services deemed critical to business continuity shall be designed with full redundancy and fault tolerance. These services shall be incorporated into the BCP – Business Continuity Plan.

Additional for PaaS solutions only:

1. Access to VMware hypervisor or HyperV Management Consoles must be restricted by ip address and/or mac addresses to a limited number of agency desktops.
2. VMware or HyperV must be configurable with virtual firewalls which can restrict access of one database to another in memory along with privileging server and application access to VM instances.

B. IAAS – INFRASTRUCTURE AS A SERVICE – [UNMANAGED HOSTED SOLUTIONS]

For IaaS Unmanaged Hosted Solutions whereby the service provider only provides space in their datacenter

1. All Primary and Backup Co-Located Data Centers must be secure and reside within the continental US.
2. Bandwidth issues concerning the Agencies internet connection and intermittent hops must be taken into consideration prior to purchasing any IaaS cloud solution space.
3. The datacenter must be secure, and meet SSAE-16 certification.
4. Review of an IaaS cloud solution requires a risk approval and the creation of a risk register followed by a high level sign off of the risk if the solution is deemed acceptable.
5. All IaaS cloud services must be vetted through the Agency's Security Accreditation process.

C. IAAS – INFRASTRUCTURE AS A SERVICE – [MANAGED HOSTED SOLUTIONS]

For IaaS Managed Hosted Solutions whereby the Service provider provides all hardware, routers, firewalls, VMware, HyperV etc.

1. Review of an IaaS cloud solution requires a risk approval and the creation of a risk register followed by a high level sign off of the risk if the solution is deemed acceptable.
2. Implementation of an IaaS cloud solution must restrict the connecting routed endpoints to a single ip address.
3. Availability and capacity requirements concerning the Agency's internet connection including intermittent hops must be taken into consideration prior to purchasing any IaaS cloud solution.
4. All IaaS cloud solutions must be vetted through the Agency's Security Accreditation process.
5. If the solution will use production data classified as *Highly Confidential*, then "N" tier encryption must be employed throughout the solution employing the *highest level of encryption possible*. This would include encryption at a minimum as follows:
   a. Encryption from the Client PC to the Web Server.
   b. Encryption from the Web Server to the Application Server.
   c. Encryption from the Application Server to the Database.
   d. It is recommended that the use of stored procedures also be encrypted where used.
   e. Production and backup databases utilized in a solution must enable column level encryption for highly confidential data in addition to encrypting data at rest utilizing Transparent Data Encryption or equivalent technologies.
6. All Primary and Backup Co-Located Data Centers must be secure and reside within the continental US.
7. The service provider must provide an operational SSAE-16 audited control document for Agency review which would include patch management and incident response along with an SLA for availability.
8. IaaS solutions must employ private cloud methodologies with single tenancy either on one physical drive, or on one logical drive utilizing virtualization with firewalls.
9. [redacted] the Agency must incorporate it's IDS, IPS, and Virus/Spyware/Malware products into the solution if not configurable by the Cloud IaaS solution.
10. A plan for degaussing or deleting data must be planned for prior to engaging in a vendor contract. A certificate of data destruction must be furnished to the agency for any and all data stores used in the solution upon termination of the contract.
11. An exit plan strategy to move data to a new vendor provider should be built into the solution.
12. The cloud provider must provide a living will if one exists.
13. Connections to all cloud services deemed critical to business continuity shall be designed with full redundancy and fault tolerance. These services shall be incorporated into the BCP – Business Continuity Plan.
14. Access to VMware hypervisor or HyperV Management Consoles must be restricted by ip address and/or mac addresses to a limited number of agency desktops.
15. All connections to management console(s) will be by https utilizing a digital certificate.
16. VMware or HyperV must be configurable with virtual firewalls which can restrict access of one database to another in memory along with privileging server and application access to VM instances.

POLICY AUTHORITY AND ENFORCEMENT

managers have a general responsibility for the implementation of this policy. users who violate this policy will be subject to disciplinary action up to and including termination of network access, loss of staff privileges, or termination of employment.

Anyone who knows or has reason to believe that another person has violated this policy should report the matter promptly to his or her supervisor, or to the Information Security Manager. All reported matters must be investigated and, where appropriate, steps taken to remedy the situation. Where possible, must make every effort to handle the reported matter confidentially. Any attempt to retaliate against a person for reporting a violation of this policy must itself be considered a violation of this policy and may result in disciplinary action.

RELATED POLICIES

Please refer to the Security Policies Cross Reference.

REVIEW OF POLICY

The policy will be reviewed annually. In the event that a significant regulatory change occurs, the policy will be updated as needed.

GLOSSARY

Please see the Glossary for a complete listing of terms used in information security policies, standards, and best practices.

DOCUMENT REVISION HISTORY

Author	Description of Change	Date of Change

DATE	DESCRIPTION
	Version 1.0 Issued.