Indiana University Public Cloud Acceptable Usage Agreement

Introduction

Security and privacy laws and other institutional policies protect much of the university's information. Before you can be granted access to the IU-sanctioned cloud computing environments, you must read and agree to follow these acceptable usage standards. You must accept responsibility for preserving the security and confidentiality of information that you store, post, access or provide access to.

Approved Cloud Platforms

As of the effective date of this document, only the following public cloud services (PaaS [1]and IaaS[2]) are approved for production use at Indiana University:

- Amazon Web Services (AWS)
- Microsoft Azure

Use of these services requires thoughtful analysis, planning, and, in many cases, governance and oversight by the management of the relevant unit, in much the same way that a unit would manage a local file server, machine room or virtual machine in the IU Data Center.

Data Classifications

NOTICE: The above listed cloud platforms are currently pre-approved for data classified as Public and University-Internal only. Any use of these cloud platforms to store, process, or transmit data that is classified as Restricted, Critical (including, but not limited to, HIPAA and PCI) **must** be specifically approved by the appropriate Data Steward(s) or responsible office (ex. Office of the Treasurer for PCI data). Additionally, a signed Business Associate Agreement (BAA) with the service provider must be in place before a unit may request Committee of Data Stewards approval for use of any protected health information (PHI) in these systems.

[1] PaaS – Platform as a Service – https://en.wikipedia.org/wiki/Platform_as_a_service
[2] IaaS – Infrastructure as a Service – https://en.wikipedia.org/wiki/Infrastructure_as_a_service

Usage Responsibilities

You agree to:

- Understand the classifications of institutional data and maintain the appropriate safeguards to protect the data. See https://datamgmt.iu.edu/types-of-data/classifications.php for details.
- Seek and receive Data Steward approval before storing, processing, or transmitting Restricted or Critical data in any of the approved cloud platforms.
- Seek updated Data Steward approvals prior to adding subsequent applications or services handling Restricted or Critical data after your Account has been established.
- For situations involving institutional data and third party applications, follow the process in Policy DM-02, Disclosing Institutional Information to Third Parties – http://policies.iu.edu/policies/categories/information-it/data-management/DM-02.shtml.
- Routinely monitor your security settings to make sure you are exposing information only to the intended audience.
- Abide by the general computing responsibilities outlined in the IU Acceptable Use Agreement – Access to Technology and Resources, available at https://ams.iu.edu/UserAgreements/HasAgreement.aspx
- Adhere to established university information and technology policies and guidelines, available at http://policies.iu.edu/policies/categories/information-it/index.shtml, including but not limited to IT-28
- Refrain from using approved cloud platforms to create shadow systems or duplicative services
- For the individual requesting the account:
    - Be responsible for any user logins or accounts created under the parent account
    - Require all users of your parent account to agree to this Indiana University Public Cloud Acceptable Usage Agreement. Maintain records of their agreement
    - Notify the Data Stewards when the make-up of the user base significantly changes
- Follow existing standards and procedures including but not limited to:
    - IU web, branding and privacy standards when hosting web sites and applications http://brand.iu.edu/
    - Standard procedures for obtaining domain names and virtual host names
    - Organizational change management processes and procedures http://change.uits.iu.edu/
    - Standards for executing web application security scans, using the appropriate vendor-provided or IU-licensed security tools https://protect.iu.edu/online-safety/tools/website-scanner.html
- Renew your account annually by reviewing and signing the current Indiana University Public Cloud Acceptable Usage Agreement and renewing the IU Purchase Order funding your accounts on the approved cloud platforms.

Important Technical Notes

At this time, UITS does not have dedicated connectivity to the approved cloud platforms nor does UITS host a centrally managed virtual data center in either cloud instance. You agree to consult with the Cloud Technology Support team (cloud@iu.edu) to assist you with making decisions about what services can best operate within the cloud environment.

Access to the approved cloud platforms will be provisioned using IU single sign on (SSO; commonly known as CAS or Shibboleth). UITS will assist in transitioning users, roles and API access to SSO for existing accounts and guiding new users on account creation.

Due to operational requirements, authorized staff from UITS, UIPO and UISO will have access to and monitor all resources hosted on the approved cloud platforms. If access is not established when resources are provisioned, access must be provided upon request. Access and monitoring by UIPO and/or UISO is not a replacement to the monitoring obligations of the unit described in this document. All security incidents, as defined in IU Policy ISPP-26 are to be reported immediately to it-incident@iu.edu.

Important Fiscal Note

Depending upon the vendor, cloud based services can be purchased as either fixed resources, or by purchasing resources only when you need them. Fixed resources lead to predictable costs. Buying resources only when needed means you are not paying for excess capacity or for CPU time when your service is not in use. However, your costs will be unpredictable and a month of heavy usage can lead to higher than budgeted costs. There are mechanisms to cap and/or monitor spending. Those tools should be used at least until you have a solid understanding of the cost of running your services.

Sanctions

Indiana University will handle reports of misuse and abuse of information and information technology resources in accordance with existing policies and procedures issued by appropriate authorities. Depending on the individual and circumstances involved this could include the offices of Human Resources, Vice Provost or Vice Chancellor of Faculties (or campus equivalent), Dean of Students (or campus equivalent), Office of the Vice President and General Counsel, and/or appropriate law enforcement agencies. See policy IT-02, Misuse and Abuse of Information Technology Resources for more detail.

Failure to comply with Indiana University information technology policies may result in sanctions relating to: the individual's use of information technology resources (such as suspension or termination of access, or removal of online material and services); the individual's employment (up to and including immediate termination of employment in accordance with applicable university policy); the individual's studies within the university (such as student discipline in accordance with applicable university policy); civil or

criminal liability; or any combination of these.

Assent

You understand and agree to the following:
Although the vendors of the approved cloud platforms apply technical safeguards to their base infrastructure, you are responsible for appropriately configuring, securing, monitoring and reporting your services. You are responsible for managing the data stored, processed, or transmitted by those services. You are responsible for following ALL applicable Indiana University policies. You are responsible for securing the necessary Data Steward approvals for the data used by the systems you build on the approved cloud platforms. You must accept these responsibilities and standards of acceptable use. By accepting these terms, you agree to follow these rules in all of your interactions with the above-listed approved cloud platforms.

Please contact the Cloud Technology Support team (cloud@iu.edu) if you have any questions about this agreement. If you choose not to accept these standards of behavior, you will be denied access to the approved cloud platforms.

I have read, understand, and agree to abide by the practices outlined in this Indiana University Public Cloud Acceptable Use Agreement.

_____ _____
Name of authorized requestor (IT Manager) Date

_____
Signature of authorized requestor (IT Manager)

_____ _____
Name of authorized requestor (functional lead) Date

_____
Signature of authorized requestor (functional lead)

Document Version 1.1 (6/13/2018)