University of Rochester
Public Cloud Acceptable Use Agreement

Contents

Purpose

Security and privacy laws and other institutional policies protect much of the university's information. Before you can be granted access to the University of Rochester's sanctioned cloud computing environments, you must read and agree to the [University's Acceptable Use Policy](). In addition, you must read and attest to this addendum which is specific to using cloud services. You must accept responsibility for preserving the security and confidentiality of information that you store, post, access or provide access to. You or your sponsor must also be able to provide a funding source for the expenses associated with the cloud services that will be consumed.

Scope

Consistent with the UR's primary Acceptable Use Policy, this Agreement applies to all users of computing resources owned or managed by the University of Rochester. Individuals covered by this Agreement include, but not limited to, University faculty and visiting faculty, physicians, staff, students, alumni, contractors, volunteers, guests or agents of the administration, and external individuals and organizations accessing network services via the University's computing facilities.

Approved Cloud Platforms

As of the effective date of this document, the following public cloud services are approved for production use at the University of Rochester under the university account:

- UR-sponsored Microsoft Azure
- UR-sponsored Amazon Web Services (AWS)

Usage Responsibilities

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 Data Center.

You agree to:

- Adhere to established university information and technology policies and guidelines including the Acceptable Use Policy and IT Security Policies.
- Take responsibility for training required for those individuals having subscription access.
- Understand the classifications of institutional data and maintain the appropriate safeguards to protect the data. See University Data Governance Guidance & Policies for details.
- Adhere to the requirements detailed in the Cloud Services Shared Responsibility Agreement (this will be a link).
- Manage data according to its appropriate risk category, and apply best practices to store, share, and manage cloud data with different risk classifications.
- Renew your account annually by reviewing and signing the current UR Public Cloud Acceptable Usage Agreement and confirming or updating the Financial Activity Object(s) (FAO), which is the grant (GR5xxxxx or expense account OP2xxxxx), funding your work.

Important Technical Note:

Reference the Public Cloud Shared Responsibilities Model for technical questions and guidance, or, consult your primary IT professional.

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 processing 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. As a user of public cloud services, you are expected to monitor and adjust spending as needed.

Sanctions

The University of Rochester 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, Senior Vice President for Health Services, Vice President for Research, Provost, Dean of Students (or campus equivalent), Office of the Vice President and General Counsel, and/or appropriate law enforcement agencies. See the University's Information Technology Policy Information Technology Policy - University IT (rochester.edu) for more detail.

Failure to comply with University of Rochester 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

Although the vendors of the approved cloud platforms apply technical safeguards to their base infrastructure, you understand and agree to the following:

- You are responsible for appropriately configuring, securing, and monitoring of your services.
- You are responsible for managing the data stored, processed, or transmitted by those services.
- You are responsible for following ALL applicable University of Rochester 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 address any questions or concerns with any policies set forth within this document to the University Information Security Office (infosec@urmc.rochester.edu). 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 University of Rochester Public Cloud Acceptable Use Agreement.

Please sign on appropriate line & return

_____   _____

Name of authorized subscription requestor (User responsible for costs)   Date

_____   _____

Name of authorized requestor (IT Manager or Technical Lead)   Date

_____   _____

Name of authorized requestor (Technical Lead)   Date

_____

FAO for service costs & fees   (SC52500 will be used)

Document Version

February 03, 2023 – Version 12
Accepted by the Research IT Governance Committee (Acceptance Date 03/31/23)