Cloud Computing – Shared Responsibility Model

Table of Contents

Purpose

To support secure and effective use of cloud resources at the University of Rochester and UR Medical Center, IT Security maintains this set of guidelines for operation of public cloud services. The purpose of this policy is to ensure that these resources are used appropriately and securely, are available to users, reliable, and used for purposes appropriate to the University's mission.

This policy is intended to describe the permitted uses of cloud services. While existing policies regarding, server security, data access and data encryption among others, are applicable to cloud environments, there are specific considerations for cloud as well as tools and services available that can be leveraged to support the maintenance of compliant environments.

This policy is not meant to supersede or replace but should be read together with other University policies.

Scope

This policy applies to all faculty, staff, and students using cloud services for University work.

General Statement – UR Cloud Shared Responsibility Model

Cloud service providers generally employ a "shared responsibility" model, in which the service provider is responsible for the security "of" the cloud, and the customer is responsible for security "in" the cloud. This makes clear that while the tools and services are available to run secure workloads in the cloud, the customer is responsible for adapting and configuring the appropriate tools for their use case.

The University of Rochester extends this model to make a distinction between the responsibilities borne by University Information Technology (IT) Core Technology teams, IT Security, and Information Systems Division (ISD) teams and the cloud account owner.

The responsibilities are broken down broadly as follows:

University IT / ISD responsibilities

- Provision new cloud accounts with best practice security controls pre-implemented (e.g., identity federation, permissions guardrails, activity logging, security event notification, resource tagging, etc.)
- Implement and maintain controls & guardrails across accounts
- Implement security incident and cost anomaly detection and notification across accounts
- Respond to new security events in cloud accounts
- Maintain incident response documentation, playbook, and post-mortem reports
- Implement configuration monitoring of cloud accounts and share results with account owners
- Perform regular vulnerability assessments of the cloud resources.

Account Owner / Researcher responsibilities

- Utilize centrally provisioned resources (e.g., virtual private networks and network security groups, machine images) whenever possible
- Keep patch level of workload environment up to date using services similar to those used for on-premise environments
- Use best practices for account access (e.g., temporary credentials and role access rather than long-lived access keys or credential sharing) whenever possible
- Participate in periodic security audit
- Respond to potential security incidents and cloud configuration findings in a timely manner
- Maintain data redundancy/backups as appropriate
- Verify annually that the Financial Activity Object(s) (FAOs) which is the grant (GR5xxxxx or expense account OP2xxxxx) assigned to the cloud expense is accurate
- Keep University IT apprised of any changes in account ownership/contacts, billing processes, or upcoming major projects that will require, University IT, or ISD involvement

Note: The above list is not exhaustive and may change over time.

Required and Recommended Cloud Security Controls

The controls listed below are within the scope of the University of Rochester's implementation of cloud policy and governance. These controls are in alignment with the University Information Security Policies and Procedures Server Security Requirements and related policies, public cloud best practices, the University of Rochester cloud shared responsibility model, and the feedback of key stakeholders within the University of Rochester.

These controls are intended to empower account holders in the areas of security and governance (including auditing, change management, and cost management). University IT Architecture will continually assess and improve support for account owners in implementing these controls. This may include automatically enabling them in some cases or offering centrally-provisioned, pre-built resources in cloud accounts to make implementation easier.

All University of Rochester Azure and AWS (cloud) account holders must implement "REQUIRED" controls to be considered compliant. It is expected that most, if not all, account holders will go beyond this required set and implement the "RECOMMENDED" controls as well.

Controls

Required

ID	Governance Objective	Required Controls
1	Manage account sprawl, increase visibility	All accounts must be provisioned as a child of the master organization account.
2	Prevent unauthorized access, protect sensitive data	Administrative access to cloud resources should be granted only to those who have a business need, and access should be removed immediately upon a users' departure. Admin access groups should be audited regularly.
3	Prevent unauthorized access, protect sensitive data	User accounts with access to root privileges must have Multifactor Authentication (MFA) enabled.
4	Protect sensitive data	All data volumes and storage accounts must be tagged with an approved data security classification. Data Security Classifications are found at: Data Security Classification Policy

5	Protect sensitive data	All data volumes and storage accounts must be encrypted with University-managed keys.
6	Prevent unauthorized access, protect sensitive data	Traffic to and from all cloud resources must be encrypted with at least Transport Layer Security 1.2 (TLS 1.2)
7	Prevent unauthorized access, protect sensitive data	Virtual networks must not peer with virtual networks in non-University of Rochester accounts unless required for business needs.
8	Attribute costs accurately, increase visibility	All resources must be labeled with approved Project, Owner, Billing, and Environment tags.
9	Protect sensitive data, increase visibility	Platform instances must have a monitoring or management agent installed. (Note cloud vendor-native agents such as Azure Defender are acceptable)
10	Prevent unauthorized access, protect sensitive data	Compute instances must not have a public network interface unless required for business needs.
11	Prevent unauthorized access, protect sensitive data	Storage accounts and volumes must not be configured to allow public access unless required for business needs.
12	Track resource utilization to ensure compliance with standards	Activity logging must be turned on for all resources and services

Recommended Controls

ID	Governance Objective	Recommended Controls
13	Prevent unauthorized access, protect sensitive data	Virtual Machine (VM) firewalls and network security groups should have only authorized ports [1] open. Certain ports are only authorized to receive traffic from approved networks.
14	Prevent unauthorized access, protect sensitive data	User, network, and compute instance access privileges should follow least-privilege principle.
15	Track resource utilization to ensure efficient usage	Resource diagnostics with logs and metrics should be enabled for all compute resources.
16	Prevent unauthorized access, protect sensitive data	Console access should occur only via federated Azure AD authentication with MFA enabled.
17	Prevent unauthorized access, protect sensitive data	Command Line Interface (CLI) access should use temporary access credentials with MFA enabled.
18	Minimize wasteful resource spending	Elastic IP addresses, storage volumes, and other instance-related resources not associated with a running instance should be released or deleted.
19	Protect sensitive data, minimize wasteful resource spending	Utilize Platform-as-a-Service resources where possible (e.g., Use Azure SQL Server versus building a VM to run MS-SQL), to reduce maintenance overhead, potential vulnerabilities, and to reduce cost.

[1] For example, only TCP port 443 (HTTPS) should be open to the world. TCP 22 (SSH) and TCP 3389/UDP 3389 (Microsoft Remote Desktop Protocol) should only be open to University of Rochester-owned subnets.

Feedback and Process for Updates

The email distribution list cloud-computing@rochester.edu is the official channel for feedback, questions, and suggestions about these guidelines for using cloud services at the University of Rochester.

IT Security commits to revisiting this document and any addenda at least annually, based on feedback from the community; new tools, services, and configuration settings made available by cloud vendors; direction from IT Leadership; and the needs of the user community.

Proposed changes will be posted to the user community through the cloud-computing distribution list for community awareness, before being presented to the Vice President for Research and IT Policy Committee for consideration and adoption.

Suspension of account:

Note: Cloud services may be suspended, with notice, if the IT Security team determines that required controls are not in place and being used. Again, it is recommended that users consider all controls for use in managing their cloud data.

Related Policies

I. University of Rochester Information Technology Policy
http://www.rochester.edu/it/policy/

II. University of Rochester Acceptable Use Policy
http://www.rochester.edu/it/policy/

III. Electronic Transfer of Protected Health Information via Facsimile and Electronic Mail
http://intranet.urmc-sh.rochester.edu/policy/hipaa/Privacy/P29.pdf

VIII. Health Insurance Portability and Accountability Act (HIPAA) Privacy and Security Policies
http://intranet.urmc-sh.rochester.edu/policy/HIPAA/PolicyManual/

Administration, Review, and Approval

Administration of this policy is assigned to ISD and University IT. Questions may be addressed to UnivITHelp at 275-2000.

Appendix 1: Revision History

Modification(s) Made	Modified By:	Date of Modification	Approver	Approval Date
Presented to IT Policy Committee		February 2023	IT Policy Committee	
Presented to Research IT Governance Committee		March 2023	Research IT Governance Committee	03/31/23