

University of Rochester

Cloud Sandbox Agreement

Contents

Purpose..... 1

Scope..... 1

Information Restrictions 1

Sandbox Use Restrictions 2

Decommissioning 2

Associated Costs 3

Assent..... 3

Appendix 1: Definitions..... 4

Purpose

To support secure and effective use of cloud resources at the University of Rochester, UR Medical Center, and affiliates, IT Security maintains this agreement for operation of the cloud sandbox environment. This agreement was developed to ensure that resources are used securely, are available to potential users, reliable, and used for purposes appropriate to the University's mission.

Before access can be granted to the University of Rochester’s sanctioned cloud computing environments, sandbox operators must read and agree to this agreement. Sandbox operators must also be able to provide a funding source for the expenses associated with the cloud services that will be consumed.

Scope

This agreement applies to any persons using the University’s cloud sandbox environment. This agreement is meant to be used in conjunction with other [University policies and agreements](#).

Information Restrictions

Sandbox users are responsible for knowing the risk classifications and handling procedures of all data they work with. Refer to the University’s [Data Security Classification Policy](#) for guidance on identifying, accessing, storing, and deleting data of all risk classifications. Sandbox users are encouraged to generate dummy data when testing in a sandbox.

Only Low risk data is acceptable for use in the sandbox environment. IT Security may, at any time, run a security scan to ensure that there is not High or Moderate risk data in your environment.

Sandbox Use Restrictions

The sandbox environment is intended only for non-production use such as proof of concepts (PoC) or prototypes. A PoC is used to show if an idea can be developed, whilst a prototype shows how it will be developed. Sandbox users are prohibited from implementing any stage of production within the sandbox environment including pilot testing. See [Appendix 1](#) for exact definitions of these terms as they apply to this document.

Software that meets any of the following criteria is considered to be in the pilot stage or beyond and is not allowed to be implemented within the sandbox environment.

1. The software accesses, modifies, or receives legitimate High or Moderate risk data.
2. The software delivers a live service to any end user, system, or software outside of the sandbox environment.
3. The software accepts data input from any person other than a sandbox user or tester.
4. The software sends data to, or attempts to change any aspect of, a production environment or production software.

Testing of software within the sandbox environment is only to be done by sandbox users or by sandbox testers. Software testing which accepts input from anyone besides a sandbox user or tester as defined in [Appendix 1](#) constitutes pilot testing and is prohibited.

Sandbox environments are strictly prohibited from connecting to the internal network. Migrating resources from the sandbox environment to non-production or production environments is also prohibited.

Decommissioning

Sandbox environments will expire after a period of 90 days at which point it will be decommissioned. Sandbox operators may also choose to decommission a sandbox environment when it is no longer in use. It is not possible to recover a decommissioned sandbox or its contents including software or data. As such, sandbox operators should ensure that all desired software and data is safely backed up outside of the sandbox prior to decommission.

Associated Costs

Usage of the sandbox environment incurs costs relative to the amount of resources used. The more processing power, storage, and time that a sandbox environment is consuming, the higher the costs associated with the sandbox. It is important to note that the sandbox operator is responsible for costs associated with the sandbox environment even if the sandbox has not been accessed or used during a given time period.

Assent

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 cloud sandbox environment.

Authorized subscription requestor (User responsible for costs)

Date

Authorized requestor (IT Manager or Technical Lead)

Date

Authorized requestor (Technical Lead)

Date

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

Appendix 1: Definitions

Within the scope of this document, the following definitions apply and supersede any alternative definition for the terms.

1. **“Sandbox”** → An isolated testing environment in which software can be run without risking the integrity of systems or software outside of it.
2. **“Sandbox Operator”** → Refers to the primary sandbox user. This is the person who requested to have a sandbox environment provisioned for their use and has primary control over the contents and operations of the environment.
3. **“Sandbox User”** → Refers to the person or persons who are in control of or are working within a given sandbox environment.
4. **“Sandbox Tester”** → Refers to any person who is permitted to assist in testing software running in a sandbox environment. This is limited to people within the university such as students or co-workers who will not be the end users and have been properly informed of the following.
 - a. The software they are interacting with is in the early stages of development within a non-production environment.
 - b. They are prohibited from submitting any legitimate high or moderate risk data.
5. **“End User”** → Within the scope of this document, this term refers to any person or system who uses or interacts with the software/system in question in order to receive/access a service or product.
6. **“Dummy Data”** → Data used for testing which conforms to the formatting standards of legitimate data while containing no real information.
 - a. Example: Rather than using a real phone number use a random string of ten digits.
7. **“Proof of Concept (PoC)”** → An initial test of software intended to validate the feasibility and functionality of a particular technology, product, or process. The main purpose is to ensure a particular concept has the potential to solve the associated problem such that further development can be justified.
8. **“Prototype”** → A rudimentary working model of a product or information system, usually built for demonstration purposes or as part of the development process. A prototype is developed after a proof of concept in order to show how the solution can or will be developed.
9. **“Pilot”** → A small-scale, limited-duration deployment of a technology, solution, or process, which is designed to test its effectiveness and identify any potential issues before rolling it out on a larger scale. A pilot is the first stage of an implementation and uses real data.