

# Remote Analysis System User Guidelines

Hirosaki University COI Data Management Committee

## 1. Purpose

This guideline aims to establish the requirements for using the remote analysis environment (hereinafter referred to as the "Remote Analysis System") operated or designated by the Hirosaki University COI Data Management Committee (hereinafter referred to as the "Data Management Committee"), and for connecting to analysis terminals located on campus or in the cloud from outside Hirosaki University via VPN or other secure communication methods approved by the Data Management Committee.

\* The Remote Analysis System includes, in addition to the Thin Telework System provided by NTT and IPA, Amazon WorkSpaces provided by Amazon Web Services, and similar services.

## 2. Eligibility for Use

Those eligible to use the Remote Analysis System (hereinafter referred to as "Users") are limited to individuals who handle data and are listed in the "Form 1: Data Analysis Application" approved by the Data Management Committee.

## 3. Application for Use

Those wishing to use the Remote Analysis System shall submit the "Form 9: Remote Analysis Use Application" to the Data Management Committee and obtain approval from the Committee.

## 4. Approval and Renewal of Use

1. The Data Management Committee shall review the application submitted under the preceding article and, if deemed appropriate, approve the use and grant the account necessary for using the Remote Analysis System.
2. The validity period of the Remote Analysis System account shall, in principle, be a maximum of three (3) months from the start date of use. However, this shall not apply in cases where the Data Management Committee individually approves otherwise.
3. Renewal of use may only be applied for within the data analysis period stated in the "Form 1: Data Analysis Application."
4. Access to the Remote Analysis System shall be limited to the approved User only.

## 5. Prohibition on Misuse and Third-Party Use of Assigned Accounts

Users shall not use the assigned account for any purpose other than those stated in the application, nor allow any third party to use it.

## 6. Restrictions on Application Use

1. Applications that may be used on the Remote Analysis System shall, in principle, be limited to those listed in and approved via the "Form 9: Remote Analysis Use Application."
2. If a new application is to be installed on the Remote Analysis System, prior application shall be submitted and permission shall be obtained from the Data Management Committee.
3. The use of applications requiring communication with external networks (the Internet) shall in

principle be prohibited. However, if unavoidable for research purposes, an application shall be submitted to request permission for the minimum necessary scope, and individual approval shall be obtained.

4. Users shall strictly comply with the license terms and conditions of each application and use them under their own responsibility.

## **7. Management of Remote Analysis Terminals**

An "access source terminal" refers to a terminal installed at the research institution or other organization to which the User belongs (outside the university) and used to connect to the Remote Analysis System. An "access destination terminal" refers to a terminal installed within the university or in the cloud, which the User connects to from an access source terminal to perform analysis and similar tasks (including Amazon WorkSpaces, etc.). Hereinafter, access source terminals and access destination terminals are collectively referred to as "Remote Analysis Terminals."

Users shall comply with the following requirements regarding the management of Remote Analysis Terminals:

1. Login IDs, passwords, authentication information, and similar credentials shall be strictly managed to prevent disclosure to others.
2. Access source terminals shall be properly stored in lockable rooms.
3. For Remote Analysis Terminals, appropriate measures shall be taken at all times to prevent infection by viruses and other unauthorized software. Additionally, the effectiveness and security of such measures shall be verified and maintained (e.g., confirming and maintaining updates to pattern files, and keeping antivirus software up to date at all times).
4. When leaving the seat while using the Remote Analysis System, the screen shall be locked. (Lock the screen: log off or use a password-protected screen saver, etc.)

## **8. Response to Security Incidents**

If any of the following circumstances arise, Users shall promptly report to the Data Management Committee:

1. If virus infection is suspected on Remote Analysis Terminals
2. If there is a possibility of unauthorized access having occurred
3. If Remote Analysis Terminals (excluding those installed in the cloud) have been stolen or lost
4. If authentication information (ID, password, etc.) may have been leaked to a third party

## **9. Revocation of Use Authorization**

The Data Management Committee may revoke the use authorization or suspend use if a User violates this guideline or the conditions of approval, or uses the Remote Analysis System for purposes other than those approved.

## **10. Disclaimer**

The Data Management Committee shall bear no responsibility whatsoever for any damages arising from the use or inability to use the Remote Analysis System (including the Thin Telework System, Amazon WorkSpaces, etc.) or related matters by Users or third parties (including damages caused by infection with viruses, malware, or similar threats, suspension, interruption, or restriction of the Remote Analysis System, malfunctions, or communication line failures).

However, this shall not apply in cases where such damage was caused by the intentional act or gross negligence of the Data Management Committee.

#### **11. Governing Language**

This document is an English translation provided for convenience only. In the event of any inconsistency or discrepancy between the Japanese version and the English version, the Japanese version shall prevail.