NBDC Security Guidelines for Human Data (for Database Center Operation Managers and "Off-Premise-Server" Operation Managers) ver. 4.0

Feb. 1,, 2024

Ver. 4.0

Introduction

The Database Center for Life Science (DBCLS) / the Joint Support-Center for Data Science Research (DS) of the Research Organization of Information and Systems (ROIS) operates the NBDC Human Database in accordance with the NBDC Guidelines for Human Data Sharing (hereinafter, the Data Sharing Guidelines). For data users, we have the NBDC Security Guidelines for Human Data (for Data Users) (hereinafter, the Data User Security Guidelines). For database centers (hereinafter, DB centers), which receive data from data submitters and offer them to data users, security measures that are stronger than those taken by data users are required because DB centers handle not only controlled-access data, which are defined in the Data Sharing Guidelines, but also data for future release (data held prior to publication of a paper or acquisition of a patent). Data handled by DB centers (hereinafter, handled data) must be assigned codes or numbers that are unrelated to the individuals in lieu of all or part of the description or the like that may lead to identification of a particular individual (including one deceased) and further assigned another set of codes or numbers.

Based on the Data User Security Guidelines, the guidelines in this document set forth the security measures to be implemented by DB centers. The "available server outside of affiliated organization (hereinafter, "off-premise-server")" defined in the Data Sharing Guidelines, which provides the data users with resources for saving and computing data, must also comply with these guidelines.

Because the information technology (IT) environments surrounding DB centers or data users are diverse and ever-changing, merely complying with these guidelines may not be sufficient for data security. Each DB center is responsible for taking additional security measures as deemed necessary. These guidelines will be updated appropriately in response to advances in IT environments.

1. Definitions

1. Controlled-access data, Data
    - The "controlled-access data" as defined in the Data Sharing Guidelines.
2. Operation manager
    - The person in charge of a DB center or an "off-premise-server".

3. Operator
    - A person who has been granted by the operation manager access to the data stored in the data server for works related to the operation of the DB center or the “off-premise-server.”
4. Data user
    - The “data user” as defined in the Data Sharing Guidelines.
5. Data server
    - A computer environment for processing such as storing and encrypting data provided by data submitters, sending controlled-access data to data users, and so on at the DB center. Alternatively, in the “off-premise-server,” a computer environment for data users to store and calculate controlled-access data.
6. Data access terminal
    - A device that is for operators to access data in the data server and that does not permanently save the data locally. When transmitting data between the data access terminal and the data server, via a communication path outside the data server-installed LAN, it is necessary that all communication paths are encrypted with sufficient strength or that the data themselves are encrypted before being transmitted.

2. Security Measures

As a general rule, measures equivalent to “3. Measures to Be Taken under High-level (Type II) Security” in the Data User Security Guideline must be implemented.

2.1 What the Operation Manager Must Do

Operation in general

1. The operation manager must operate in compliance with the Data Sharing Guidelines and the NBDC Security Guidelines for Human Data.
2. The operation manager should create a list of operators and keep it up-to-date at all times.
3. The operation manager should make the operators fully understand and comply with the NBDC Security Guidelines for Human Data.
4. The operation manager should receive an education on information security implemented by the affiliated or equivalent organization, and have all operators receive the same education.

5. The operation manager should keep a record of information on the operators and the data server (including the storage location in the file system) in an electronic file or the like accessible only to the operation manager and the operators, and update the record every time a change occurs. The record should be managed so that the update history can be reviewed.
6. The operation manager should accept an audit conducted by the DBCLS or a third party commissioned by the DBCLS with regard to the state of implementation of security measures.
7. The operation manager should voluntarily perform audits by system security experts at the time of system construction and every two to three years. A copy of the audit result should be submitted to the DBCLS.
8. In case of a security incident such as data breach, the operation manager must immediately take measures and promptly report the incident to the DBCLS.

Data Server

1. The operation manager should place the data server in a server room that meets all of the following requirements (1) to (3).
    - (1) Access to the room is limited using multi-factorial authentication with at least two of the following three authentication methods.
        - Biometric authentication (e.g., vein, fingerprint, iris, and face recognition)
        - Property-based authentication (e.g., IC card, one-time password, and USB token)
        - Knowledge -based authentication (e.g., password)
    - (2) Record of access to the room is automatically obtained and made available for later audit.
    - (3) The server room must be dedicated to this purpose. If a dedicated server room cannot be set up, the data server must be stored in a locked dedicated server rack.
2. The operation manager should control the access to/from the data storage area of the data server and the area that the data users use for data storage and calculation appropriately. It is necessary to manage so that only operators and data users can access only authorized data via the data server or the Internet.

3. The operation manager should install a firewall between the LAN where the data server is installed and the external network, and manage the access to/from the outside to the minimum necessary (e.g., the IP address and port of source and destination are limited) to keep high security.
4. The operation manager should restrict even communication from/to the LAN where the data server is installed appropriately at least by a firewall function (e.g., iptables in Linux) provided by the OS etc.
5. The operation manager should not allow sharing of a user ID or a password for the data server among data users, and have them set the password to a sufficient strength that others cannot guess. (It must be at least 8 characters. Combination of numbers, upper case letters, lower case letters, and symbols is preferable. Do not use that are easy to guess such as name, phone number, birthday, and the like.)
6. The operation manager should apply the latest security patches insofar as possible for all software installed on the data server.
7. The operation manager should not install software unnecessary for service, particularly, file sharing software (also called file exchange or P2P software; e.g., Winny, BitTorrent).
8. The operation manager should install antivirus software and perform virus scan at once whenever incorporating a data file other than the one which was downloaded from the Japanese Genotype-phenotype Archive (JGA), the DDBJ Sequence Read Archive(DRA), and the Genomic Expression Archive (GEA), from the outside of the data server. The operation manager must keep the antivirus software and virus definition file up to date.
9. The operation manager should not start unnecessary processes as many as possible when the OS boots up etc.
10. The operation manager should acquire the access log of the data server and check it regularly.
11. When discarding a device that stored handled data, the operation manager should initialize the data storage area or physically destroyed in a way that cannot be restored.
12. In case of a security incident such as data breach, the operation manager should immediately take measures.

2.2 What the Operator Must Do

1. The operator should receive an education on information security implemented by the affiliated organization and the like.
2. When logging in to the data server from a data access terminal via communication paths outside the LAN where the data server is installed, the operator should encrypt all the

communication paths using a sufficiently strong encryption method every time data are transmitted between the data access terminal and the data server or encrypt the data themselves before transmitting them. It is desirable to perform similar encryption even when logging in to the data server from the inside of the LAN where the data server is installed.

3. The operator should not access data from a terminal application on a device that can be used by many and unspecified persons (e.g., a PC in an Internet cafe).
4. The operator should apply the latest security patches to the data access terminal whenever possible.
5. When leaving a data access terminal, the operator should log out from the data server or lock the terminal. In addition, the terminal should be configured so that the screen is locked after a certain period of inactivity (around 15 minutes).
6. The operator should not access data that he/she does not have permission from the Operation manager or data user.
7. The operator should not copy or save handled data displayed on a data access terminal screen to the local disk. It is desirable to use a data access terminal application that does not permit copying and saving of handled data displayed on the terminal screen to the local disk.
8. The operator should disable a cache function which automatically saves data on the data access terminal.
9. The operator should not make copies of handled data or move handled data outside the data server, except in the following cases. In these cases, delete the copies promptly after use in a way that cannot be recovered.
    - Creation of a backup copy of handled data
    - Temporary duplication at the time of transfer of handled data
    - Temporary duplication performed by software
10. When obtaining a backup data, the operator should ensure that one of the following requirements is met.
    - The backup is saved on the data server.
    - When the backup is saved in a mobile device (e.g., a tape, USB memory, CD-ROM, notebook PC), the handled data is encrypted and deleted after use in a way that does not allow restoration. A record of information regarding the mobile device and the backed-up handled data should be kept in the file described in the section “2.1 What the Operation Manager Must

Do," Operation in general, item (5), to minimize the risk of theft or loss and to enable early detection when such an incident occurred.

11. When it is inevitable to use a mobile device for temporary data transfer, the operator should handle the data in the same way as backup data.
12. When it is inevitable to print handled data out, the operator should strictly manage the printout to protect confidentiality of the data, and shred the printout after use.
13. In case of a security incident such as data breach, the operator should immediately take measures and report the incident to the operation manager.

Be noted the above items (9) to (12) are not applied to the "off-premise-server."