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

NBDC Security Guidelines for Group Sharing Human Data (for Database Center Operation Managers and "Off-Premise-Server" Operation Managers)

2024/4 Ver.4.0

All Mark Hard Department Namesger Name (appears on completives as in the loss) Sharing Scaledous and in Name (as a second scale of the loss) Sharing Scaledous and in Name (as a second scale of the loss) Sharing Scaledous and in Name (as a second scale of the loss) Sharing Scaledous and Interest Name (as a second scale of the loss) Sharing Scaledous and Interest Name (as a second scale of the loss) Sharing Scaledous and Interest Name (as a second scale of the loss) Sharing Scaledous and Interest Name (as a second scale of the loss) Sharing Scaledous and Interest Name (as a second scale of the loss) Sharing Scaledous and Interest Name (as a second scale of the loss) Sharing Scaledous and Interest Name (as a second scale of the loss) Sharing Scaledous and Interest Name (as a second scale of the loss) Sharing Scaledous and Interest Name (as a second scale of the loss) Sharing Scaledous and Interest Name (as a second scale of the loss) Sharing Scaledous and Interest Name (as a second scale of the loss) Sharing Scaledous and Interest Name (as a second scale of the loss) Sharing Scaledous and Interest Name (as a second scale of the loss) Sharing Scaledous and Interest Name (as a second scale of the loss) Sharing Scaledous and Interest Name (as a second scale of the loss) Sharing Scaledous and Interest Name (as a second scale of the loss) Sharing Scaledous and Interest Name (as a second scale of the loss) Sharing Scaledous and Interest Name (as a second scale of the loss) Sharing Scaledous and Interest Name (as a second scale of the loss) Sharing Scaledous and Interest Name (as a second scale of the loss) Sharing Scaledous and Interest Name (as a second scale of the loss) Sharing Scaledous and Interest Name (as a second scale of the loss) Sharing Scaledous and Interest Name (as a second scale of the loss) Sharing Scaledous and Interest Name (as a second scale of the loss) Sharing Scaledous and Interest Name (as a second scaledous scaledous scaledous scaledous scaledous and Interest Name (as a second scaledous scaledo	If infeasible, state the reason	State of compliance	Requirements	lause umber
### Secretary Name of Processing Secretary Sec			urity Measures	Security M
Secondary in parents				
sequence in mercage and improvement completation can be in the Care Strong (Survivine and the MICC). Counting Guidenters for these Date of Group Strong Strong Strong Counting				
The control or multiple review (article) is fell dispensation of the control of t				
The opportunit managery are search managery and account and an analysis price in the March 19 for Search 19 of Search 19 o		Possible	The operation manager must operate in compliance with the Data Sharing Guidelines and the NBDC Security Guidelines for Human Data / for Group Sharing Human Data.	1
A to repertine manager desired near the content of a search production and production of the content of the repertine manager desired the content of the con		Possible	The operation manager should create a list of operators and keep it up-to-date at all times.	2
The quantition remarging which the part amount of inflammation in the quantition, and production in the first production in the first production in the first production in the part of th		Possible	The operation manager should make the operators fully understand and comply with the NBDC Security Guidelines for Human Data / for Group Sharing Human Data.	3
Security of the control of the control in the control into control int				
Page coast of a coast of the co		Possible	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.	5
Page 1 as accurry modern such as doub bream, the operation manager most immediately bits measures and promptly report the modern to the Districts. Propulary for accurate the propular of the				6
Data Service The operation manager decide place the data core in a lover come that meats at if the Solaring expariments (1) (-2)		P.ossible	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 DBC	7
The operation manager should place the date server is a server room that in feet and of the fibrowing experiments (1) (c) (c) (c) (c) (c) (c) (c) (c) (c) (c		Possible	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.	8
11) Accesses to the room is limited using multi-fickations with effective tow of the foliawing times extination for a part administration (e.g., password) 12) Accessed and administration (e.g., password) 13) Call Room of a disease to the room of a subministration (e.g., password) 14) Call Room of a disease to the room of a subministration (e.g., password) 15) This can've mean must be additional to the purpose if it is distributed for their suit. 16) This can've mean must be additional to the purpose if it is distributed for their suit. 17) This can've mean must be additional to the purpose if it is distributed for the room of the room of the distributed for the room of the room o			erver	ata Server
has only operations and data users can access only authorized data valle data server is installed appropriately at least by a frewalf function (e.g., ipsibles in Linux) provided by the OS etc. The operation manager should not a least feature between the LAM where the data server is installed appropriately at least by a frewalf function (e.g., ipsibles in Linux) provided by the OS etc. Provided the provided of a least of the common of the Common of the LAM where the data server is installed appropriately at least by a frewalf function (e.g., ipsibles in Linux) provided by the OS etc. Provided the Common of the Common of the LAM where the data server is installed appropriately at least by a frewalf function (e.g., ipsibles in Linux) provided by the OS etc. Provided the Common of the Common of the LAM where the data server is installed appropriately at least by a frewalf function (e.g., ipsibles in Linux) provided by the OS etc. Provided the Common of the Common of the Common of the LAM where the data server is installed appropriately at least by a frewalf function (e.g., ipsibles in Linux) provided by the OS etc. Provided the Common of the Common of the Common of the Common of the LAM where the data server is installed appropriately at least by a frewalf function (e.g., ipsibles in Linux) provided by the LAM where the Common of the LAM where the Co		Possible	(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.	1
softenes and port of source and destination are limited) to keep high security. The operation manager personal manager should around story a few provided by the OS etc. The operation manager should 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 disposed to the control of the control		Bo ssible		
Software story or Souther all not described and constrainant are timedy to keep high Security. 4 The operation manager should story that sharing of a user? Or a password for the data server as intelliged appropriately at least by a flewward function (e.g., uptables in Linux) provided by the OS etc. 5 The operation manager should story the latest security puthers involved an appropriately as the story of	-	Possible		
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 thesable least of 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 install at sinchina shortware unnecessary for sexe, particularly, first behang software (also called the sechange or PZP achievire; e.g., Winny, Biff orreit). 7 The operation manager should not install a shortware unnecessary for sexe, particularly, first behang software (also called the sechange or PZP achievire; e.g., Winny, Biff orreit). 8 Archive (CAC), the DDIS Supperson Read Archive (CPA), and the Genomic Expression Archive (CPA), the DDIS Supperson Read Read Read Read Read Read Read Read			address and port of source and destination are limited) to keep nigh security.	3
least 8 characters. Combination of numbers, upper case letters, and symbols is preferable. Don not use that are easy to guess such as name, phone number, birthday, and the like.) 6 The operation manager should not install software unaccessary for service, particularly, file sharing software (sides called file exchange or P2P software, e.g., Winny, BiT cremt). 7 The operation manager should not install software unaccessary for service, particularly, file sharing software (sides called file exchange or P2P software, e.g., Winny, BiT cremt). 8 destruct (EA), the DDS Sequence Read Archive (PRA), and the Genomic Expression Archive (CEA), 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 staff unnecessary processes as many as possible when the CS bods up sic. 10 The operation manager should and staff unnecessary processes as many as possible when the CS bods up sic. 11 When decarding a device that stored handled dails, the operation manager should intellect the data server. The operation manager must keep the antivirus software and virus definition file up to date. 12 In case of a security incident out and a staff unnecessary processes as many as possible with the CS bods up sic. 13 The operation manager should and handled dails, the operation manager should intellect the data staff unnecessary processes as many as possible with the community of the staff unnecessary processes as many as possible with the community of the staff unnecessary processes as many as possible with the community of the staff unnecessary processes as many as possible with the community of the staff unnecessary processes as many as possible with the community of the staff unnecessary processes as many as possible with the community of the staff unnecessary as the staff unnecessary of the staff unnecessary processes as many as possible with the community of the staff unnecessary as the staff unnecessary as the staff unneces		Possible	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.	4
The operation manager should not install software unnecessary for service, particularly, file sharing software (aloc called file exchange or PZP software, e.g., Wirry, Bill Torrent). Possible The operation manager should not install software unnecessary processes as many as possible when the Operation file up to date. 9 The operation manager should not start unnecessary processes as many as possible when the OS boots up etc. 9 The operation manager should acquire the access log of the data server and check it regularly. 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 into manager should into manager should into manager should into manager should into the should be should be should be should be should should be should		Prossible	least 0 shows story Combination of numbers, upper seed letters, leaves and symbols in referable. Do not use that are easy to guess such as now, where number highest and the like \	la la
The operation manager should intail antivirus software and perform virus scan at once whenever incorporating a data file other than the one which was downloaded from the Japanese Cenchyle-Chenchyle 8 Arthory (CAR), the DBJS Sequence Read Archive (DRA), and the Genomic Expression Archive (CEA), from the outside of the data server. The operation manager must keep the antivirus software and virus 9 The operation manager should acquire the access tog of the data server and check it regularly. 9 The operation manager should acquire the access tog of the data server and check it regularly. 10 The operation manager should acquire the access tog 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 initialize the data storage area or physically destroyed in a way that cannot be restored. 12 Possible 12 Possible 12 Possible 13 The operator Must DO 14 The operator should receive an education on information security implemented by the affiliated organization and the like. 15 When togging in to the data server from a data access terminal via communication paths using a sufficiently storing encryption method every time data are transmitted between the data access terminal and the data server or encrypt the data themselves before transmiting them. It is desirable to perform similar encryption even then fologing in to the data server from the inside of the LAW where the data server rein installed. 15 The operator should not access data from a terminal application on a device that the third every installed. 16 The operator should not access data from a terminal application on a device that access terminal access terminal. In addition, the terminal should be configured so that the screen is locked after a certain period of possible 17 The operator should not access data		Possible	The operation manager should apply the latest security patches insofar as possible for all software installed on the data server.	6
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 tog of the data server and check it regularly. Possible 11 When discarding a device that stored handed data, the operation manager should intilizate the data storage area or physically destroyed in a way that cannot be restored. Possible 12 In case of a security incident such as data breach, the operation manager should inmediately take measures. 22 What the Operator Must DO 1 The operator should receive an education on information security implemented by the affiliated organization and the like. When logging in to the data server from a data access terminal via communication paths outsign a sufficiently strong encyption method every time data access terminal and the data server or encypt the data fhemselves 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 cases 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). Possible 1 The operator should access data that he final the data server is installed. 1 The operator should for a cases 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). Possible 1 The operator should in a cases data that he final the data server is installed. 1 The operator should in a case start of the data access terminal stream of the data server is installed. 1 The operator should compare the data server is the data server is compared to the data server is installed. 2 The operator should data that the se		Possible	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).	7
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 imbulative the data storage area or physically destroyed in a way that cannot be restored. 22 What the Operator Must Do 1 The operator should receive an education on information security implemented by the affiliated organization and the like. 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 like. 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 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). 9 When leaving a data access terminal, the operator should on to access data that he/she does not have permission from the Operation manager or data user. 7 In 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 Rdssible handled data displayed on the terminal screen to the local disk. It is desirable to use a data access terminal application that does not permit copying and saving Rdssible 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 Rdssible handled data displayed on a data access terminal screen to the local disk. It is desirable to use a data access terminal applica		Possible	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	8
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. Possible 12 In case of a security incident such as data breach, the operation manager should immediately take measures. Possible 1 The operator should receive an education on information security implemented by the affiliated organization and the like. When logging in to the data server from a data access terminal via communication paths outside the LAN where the data server or encrypt the data the retransmitted between the data access terminal and easier or encrypt the data the retransmitted between the data access terminal and the like. 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. When leaving a data access terminal, the operator should log out from the data server or lock the terminal should be configured so that the screen is locked after a certain period of some control of the possible in the operator should not access data that he/she does not have permission from the Operation manager or data user. Possible The operator should not cocy 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 dissible handled data displayed on the terminal screen to the local disk. The operator should not cory or save handled data displayed on a data access terminal screen to the local disk. The operator should into the access of handled data access terminal screen to the local disk. The operator should not make copies of handled data access terminal screen to the local disk. The operator should not make copies of handled data access terminal screen to the local disk. The operator should not make cop		Possible	The operation manager should not start unnecessary processes as many as possible when the OS boots up etc.	9
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. 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 secret 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 In the leaving of data access terminal whenever possible. 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 access data that he/she does not have permission from the Operation manager or data user. 7 The operator should not access data that he/she does not have permission from the Operation manager or data user. 8 The operator should not access data that he/she does not have permission from the Operation manager or data user. 9 Possible 1 The operator should not access data that he/she does not have permission from the Operation manager or data user. 1 The operator should not access data that he/she does not have permission from the Operation manager or data user. 2 Possible 3 The operator should not access data that he/she does not have permission from the Operation manager or data user. 4 The operator should not access data that he/she does not have permission from the Operation manager or data user. 5 The operator should disable a cache function which automatically saves data on the data access terminal period of the data decretion of the data every control of the data every con		Possible	The operation manager should acquire the access log of the data server and check it regularly.	10
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 sever 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 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 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 data servers in installed. 3 The operator should not access data from a terminal application on a device that can be used by many and use performance in the operator should popt by the latest security patches to the data access terminal whenever possible. 4 The operator should apply the latest security patches to the data access terminal whenever possible. 5 In the operator should not access data that he/she does not have permission from the Operation manager or data user. 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 access data that he/she does not have permission from the Operation manager or data user. 8 The operator should not access data that he/she does not ada access terminal splication that does not permit copying and saving access the operator should not make copies of handled data outside the data access terminal. The operator should not make copies of handled data or move handled data outside the da				
The operator should receive an education on information security implemented by the affiliated organization and the like. When logging in to the data server from a data access terminal via communication paths outside the LAN where 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 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). Possible The operator should apply the latest security patches to the data access terminal whenever possible. Possible 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). The operator should not access data that he/she does not have permission from the Operation manager or data user. 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 disable a cache function which automatically saves data on the data server, except in the following cases. In these cases, delete the copies promptly after use in a way that cannot be recovered. The operator should not make copies of 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. The operator should not make copies of handled data Temporary duplication performed by software When obtaining a backup data, the operator should ensure		Possible	In case of a security incident such as data breach, the operation manager should immediately take measures.	12
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 went when logging in to the data server in 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. When leaving a data access terminal, the operator should log out from the data server or lock the terminal should be configured so that the screen is locked after a certain period of linactivity (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 savingted sistile. 8 The operator should installe a cache function which automatically saves data on the data access terminal. The operator should in the time of transfer of handled data or move handled data or envel handled			at the Operator Must Do	2 What the
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 Interview of the person of 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 possible interview of the person of the person of the person of the terminal should be configured so that the screen is locked after a certain period of possible interview of the person of the person of the person of the terminal strong of the person of the screen is locked after a certain period of possible interview of the person of the person of the terminal strong of the person of the person of the terminal strong of the person of the person of the terminal strong of the person of				
The operator should apply the latest security patches to the data access terminal whenever possible. 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). The operator should not access data that he/she does not have permission from the Operation manager or data user. The operator should not opy 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 dissible handled data displayed on the terminal screen to the local disk. The operator should disable a cache function which automatically saves data on the data access terminal. 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 at the time of transfer of handled data Temporary duplication performed by software 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 obtaining a backup data, the operator should ensure that one of the following requirements is met. The backup is saved on the data server that data server that one of the following requirements is met. The backup is saved on the data server that one of the following requirements is met. 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 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 obtaining a backup data, the op		Possible	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	2
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 for said and 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. 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. 9 - Creation of a backup copy of handled data - Temporary duplication at the time of transfer of handled data - Temporary duplication at the time of transfer of handled data - Temporary duplication performed by software When obtaining a backup data, the operator should ensure that one of the following requirements is met. 10 - 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.		Possible		-
5 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 Rdssible handled data displayed on the terminal screen to the local disk. It is desirable to use a data access terminal application that does not permit copying and saving Rdssible handled data displayed on the terminal screen to the local disk. It is desirable to use a data access terminal application that does not permit copying and saving Rdssible handled data displayed on the data screen to the local disk. It is desirable to use a data access terminal application that does not permit copying and saving Rdssible handled data access terminal application that does not permit copying and saving Rdssible handled data access terminal application that does not permit copying and saving Rdssible handled data access terminal application that does not permit copying and saving Rdssible handled data access terminal application that does not permit copying and saving Rdssible handled access terminal application that does not permit copying and saving Rdssible handled data access terminal application that does not permit copying and saving Rdssible handled access terminal application that does not permit copying and saving Rdssible handled data server in the following requirements is met. 9 Creation of a backup copy of handled data access terminal application that does not permit copying and saving Rdssible handled data access terminal application that does not permit copying and saving Rdssible handled access terminal application that does not permit copying and saving Rdssible handled access terminal application that does not permit copying and saving Rdssible handled access terminal application that does not permit copying and saving Rdssible handled access ter	·		1 112	-
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 Rdssible handled data displayed on the terminal screen to the local disk. The operator should disable a cache function which automatically saves data on the data access terminal. 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. 9 - Creation of a backup copy of handled data - Temporary duplication at the time of transfer of handled data - Temporary duplication performed by software 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.		Possible		5 i
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. 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. 9 - Creation of a backup copy of handled data - Temporary duplication at the time of transfer of handled data - Temporary duplication performed by software 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. 10 - 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.				ŭ
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. 9		Rufssible		
recovered. 9 - Creation of a backup copy of handled data - Temporary duplication at the time of transfer of handled data - Temporary duplication performed by software 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. 10 - 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.		Possible	The operator should disable a cache function which automatically saves data on the data access terminal.	8
9 - Creation of a backup copy of handled data - Temporary duplication at the time of transfer of handled data - Temporary duplication performed by software 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. 10 - 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.		Possible		
- The backup is saved on the data server. 10 - 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.			- Creation of a backup copy of handled data - Temporary duplication at the time of transfer of handled data - Temporary duplication performed by software	9 -
When it is inevitable to use a mobile device for temporary data transfer, the operator should handle the data in the same way as backun data Possible			- 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 minim	10 - i
11 Composition of the position		Possible	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.	11
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."		Possible		

Date
Date
Division of the principal investigator(PI)
Research Organization of Information and Systems, National Institute of Genetics Bioinformation and DDBJ Center
Name of PI
Osamu Ogasawara

* The information provided on this checklist will never be used for purposes other than the review conducted by the Human Data Rev