|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  |  | |  | | --- | | DBGAP Data Security PLAN | |  | |

# PHYSICAL SECURITY

|  |  |
| --- | --- |
|  | Identify all systems involved in storing, transmitting, and analyzing dbGaP data, including physical location.  **Systems:** |
|  | **Best practice:** Restrict physical access to all servers, network hardware, storage arrays, firewalls and backup media only to those that are required for efficient operations.  **Describe measures taken:** |
|  | **Best practice**: Log access to secure facilities, ideally with electronic authentication.  **Describe measures taken:** |

# INFORMATION SECURITY

|  |  |
| --- | --- |
|  | **Best practice:** Make sure controlled files are never exposed to the Internet with the exception of such connections as are required to download data from source repositories. Infrastructure should be behind local and/or institutional firewalls that block access from outside of the institution.  **Describe measures taken:** |
|  | **Best practice:** Ensure that your security profile is configured to allow access only to the minimum set of ports required to provide necessary functionality for your services and limit access to specific networks or hosts. In addition, allow administrative access only to the minimum set of ports and source IP address ranges  **Describe measures taken:** |
|  | **Best practice:** Utilize strong authentication technology for access control. Two factor authentication technologies (smart cards, hard or soft token, etc.) are preferred. Otherwise, minimum 12 character passwords changed every 120 days.  **Describe measures taken:** |
|  | **Best practice:** If accessing systems remotely, use encrypted data access (such as Secure Shell (SSH) or Virtual Private Network (VPN)).  **Describe measures taken:** |
|  | **Best practice:** Ensure that data is accessible only to those approved for access, and controls for changing that access are retained by the investigator who submitted the DAR and the appropriate IT staff. A mechanism for monitoring and notification needs to be in place to monitor permission changes.  **Describe measures taken:** |
|  | **Best practice:** Provide appropriate logging on machines where data are resident. Ensure that account access is logged along with access controls and file access.  **Describe measures taken:** |
|  | **Best practice:** Keep all software patches up-to-date  **Describe measures taken:** |
|  | **Best practice**: Disable unnecessary services on servers. Begin with a server image that disables all non-essential services and then restore those that are needed.  **Describe measures taken:** |
|  | **Best practice**: Enforce principle of Least Privilege to ensure that individuals and/or processes grant only the rights and permissions to perform their assigned tasks and functions, but no more.  **Describe measures taken:** |
|  | **Best practice:** Secure controlled-access genomic and phenotypic data on the systems from other users (restrict directory permissions to only the owner and group)  **Describe measures taken:** |
|  | **Best practice:** Ensure that data access policies are retained throughout the processing of the data on all systems (such as compute clusters). If data is cached on local systems, directory protection must be kept, and data must be removed when processing is complete.  **Describe measures taken:** |
|  | **Best practice:** Review the Access Control Lists (ACLs), permissions, and security perimeter to ensure consistent definition.  **Describe measures taken:** |

# Education and Training

|  |  |
| --- | --- |
|  | Require all users of controlled data to attend information sessions explaining security best practices before being given access to controlled data. |
|  | Post best practices clearly on websites and online documentation associated with the project. |

# Project personnel

|  |  |
| --- | --- |
|  | Identify every person (name, institution, project role) who will have access to controlled data: |

# Evaluation and review

|  |  |
| --- | --- |
|  | Every 6 months review security practices with responsible individuals to ensure that these policies are being followed and working well. Make any needed adjustments to the security plan and implementation. |