Data Protection LifeCycle

JHSPH is committed to protecting all data that has been created by its faculty, staff, students, collaborators; and all data that has been entrusted to us.

Data owners are accountable for the protection of data. Responsibility can be delegated to custodians, but accountability remains with data owners.

Protection strategies should address the **Integrity**, **Availability**, and **Confidentiality** of data.

Data protection must extend to every stage of the data lifecycle.

Risks associated with data cannot be eliminated. The goal of data protection is to mitigate risk using appropriate controls until the risk has been reduced to a level acceptable to the data owner.

While developing a data security plans, please reference the "Data LifeCycle Key Considerations" to ensure that all aspects of data protection have been addressed.

Several of the Data Lifecycle Key Considerations reference a common set of reasonable controls. To avoid duplication, these recommended minimum controls are listed here…

Reasonable Controls

- Data is encrypted in transit
  (*Here is a great explanation of how encryption works… https://www.youtube.com/watch?v=ZghMPWGXexs*)
- Data is encrypted while "at rest" (on a storage device)
- Security patches and updates are routinely applied to computing and storage devices.
- Devices have access controls so that…
  - Each person accessing the device is uniquely identified (username)
  - Passwords are sufficiently strong to prevent compromise
  - All access is logged and recorded
  - Unauthorized access is prevented
  - Approved access list is reviewed periodically for correctness

Data Lifecycle Key Considerations

Collection

- Ensure that there are *reasonable controls* on the device(s) that are being used for collection or data origination.
- Ensure that a data backup or replication strategy is in place (if permitted) to recover data in the event of a loss of the collection device(s).

Storage

- Ensure that there are *reasonable controls* on all device(s) that are being used for storage.
- Implement physical protections against theft, loss, or interference with the device.
- Ensure that a data backup or replication strategy is in place (if permitted) to recover data in the event of a loss of the storage device, or destruction of data.

Transfer

- Ensure positive confirmation of the source and destination of the data.
- Ensure data is encrypted in transit.
- Ensure positive confirmation of the complete and successful transfer of data.
- If the intent of the transfer was to "move" the data (resulting in there being one copy at the destination) confirm that the data was removed from the source following the transfer?
- If the intent of the transfer was to "copy" data (resulting in there being separate copies in both the source and destinations) confirm that data protection plan includes ongoing protection of BOTH copies through remainder of their respective lifecycles.

Sharing

- If data is being shared by providing a copy of, or a subset of them, ensure that data protection plan includes ongoing protection of BOTH copies through remainder of their respective lifecycles.
- If permissions are being granted to data at rest, ensure that *reasonable controls* (access controls) are in place.

Processing

- Ensure that there are *reasonable controls* on the device(s) that are being used for data processing.

Archiving

- Confirm removal of working sets of data from all necessary storage devices and computers.
- Ensure that *reasonable controls* are in place for the archival media being used.

Destroying

- Ensure that destruction complies with current NIST or DoD standards.
- Endure that all copies of data have been included in data destruction.