Policy 5.10 and 5.3

Policy 5.10: Cornell University expects all institutional information stewards and custodians who have access to and responsibilities for institutional information to manage it according to the rules regarding storage, disclosure, access, classification of information and minimum privacy and security standards as set forth in this policy.

- Policy 5.10
- Policy 5.10 Summary

Policy 5.3: Custodians or users of institutional administrative data who deploy software or algorithmic programs for encryption must establish procedures ensuring that the university has access to all such records and data.

- Policy 5.3
- Policy 5.3 Summary

Confidential Data

In keeping with Cornell policies, eliminating confidential data stored on Cornell and personal machines will reduce the risk that the data will be misused causing loss of reputation and financial liability to Cornell University.

- DFA Data Stewardship and Custodianship
- http://www.it.cornell.edu/policies/

Individual community members and departments are responsible for their own data security. The ITSG provides the following tools and guides to assist in your attestation.

Data Clean Up Goals

1. Scan all computers, devices and shared file server space for confidential data. Manually inspect files for confidential data that may not be found by automated scanners.
2. Eliminate or properly secure all confidential data to reduce risk of data misuse.
3. Annually attest that you have completed your inspection, and if any confidential data was discovered, it has been deleted or appropriately secured.

How Do I Get Started?

1. If you don't already have Identity Finder/Spirion on your machine, please submit a ticket to let us know.
2. Put time aside on your calendar within the next few weeks. Start the Identity Finder scan when you leave for the day. When you return the next morning, spend 30 minutes to an hour purging everything you can.
   Instructions on how to Run Identity Finder/Spirion are available.
3. Coordinate with co-workers and ITSG to not duplicate effort on scanning shared file storage space.
4. Manually inspect files that may contain confidential data but were not identified by the scan.
5. If you know there is confidential data in a file, consider deleting the file or at least the sensitive information it contains. If you must retain the information for business reasons, please submit a ticket to request assistance with securing the data.
6. Attest that you have completed your cleanup effort no later than your departmental deadline. Your link to the attestation is unique to you.

Considerations

Cornell University Policy 5.10 - Security of Electronic University Administrative Information.pdf identifies the following data elements as "confidential data" when they appear in conjunction with an individual’s name or other personal identifier.

- Social Security numbers
- Credit card numbers
- Driver's license numbers
- Bank account numbers
- Patient treatment information

What is the data retention policy for your business data?
Consider removing data that is older than regulations require.

Who owns or is responsible for the data?
Pay attention to data that may be orphaned by former co-workers or programs that have ended or no longer exist. Is there still value to retaining this data?

When was the last time the information was used?
Consider whether to keep information from old programs that are no longer in existence. Are there files on a shared server left over from former co-workers that can be reorganized or deleted?

Is the information duplicated or does it exist in other locations or systems?
Consider consolidating information so it is stored in only one place. This will allow for better data organization and reduce the time spent searching for relevant information.

If you lost the data, what would mean to the continuation of business?
Delete files you may never use. Pressing delete is just as difficult for digital hoarders as throwing items in the trash can is for traditional hoarders. Consider whether the data would actually be necessary to continue business versus feeling that the data might "someday" be useful.

What if I accidentally delete something I need?
Most computers and servers are backed up nightly. Submit a ticket with the deleted file name and it's previous location.

Data Security Plan (DSP)

If your research involves sharing data with an entity outside Cornell, you may be asked engage in a Data Use Agreement with that entity. This agreement will likely require a Data Security Plan that will be reviewed through the Office of Sponsored Programs and/or Institutional Review Board. If you have need of a Data Security Plan and haven't developed one before, please submit an ITSG Help Ticket (https://help.coecis.cornell.edu/) and we can assist you in creating one.

A data security plan (DSP) is a document that lays out the plan for obtaining, storing, backing up and recovering (if needed), protecting, and controlling and allowing access to electronic data provided to Cornell faculty, staff and (perhaps) students, from an external entity for research purposes, or in other situations where there is institutional concern about the availability and security of the data.

A Data Security Plan may be required by the Cornell Institutional Review Board (IRB) as part of the overall Research approval process. A DSP may also be part of the grant application, approval, and submission process through the Office of Sponsored Programs.

Many, if not most, other universities, commercial enterprises and research organizations will have a Data Use Agreement (DUA) that must be agreed to in order to obtain data that they will share with Cornell. A DUA is not a Data Security Plan, but the DSP must take into account and satisfy the requirements that are specified in a DUA.
The reason for preparing a written DSP is to have the data security related procedures in one document which is available to a wide range of Cornell offices. The guiding principle is that once the data is obtained for Cornell, it “becomes” Cornell data – Cornell is now the responsible party for data security, sharing, use in research and publications, etc. Thus the data is not only regulated according to any Data Use Agreement, but also by Cornell’s own IT Data Security Policies.

All electronic data at the university falls generally under IT Security Policy 5.10. The applicant/plan author should make themselves familiar with Policy 5.10. This policy may be accessed here: https://www.dfa.cornell.edu/sites/default/files/vol5_10.pdf

A major part of the DSP is the correct classification of the data to be stored. Policy 5.10 recognizes 3 levels of data: public, restricted, and confidential. Confidential data has the strictest storage and use requirements; it includes HIPAA data, and data related to personal and financial information. HIPAA data storage is available only through special arrangement, and other financial data may only be stored through the Cornell Restricted Access Data Center (CRADC). COECIS/ITSG does not support any individual facilities for, or handling of, confidential data.

Restricted data is all other data used in the conduct of university business which is not public data. Cornell research data is specifically excluded from coverage by this classification, but the Data Use Agreements required by the external owner of the data demand that the data be restricted. Thus, most shared research data would probably be considered to be in this category. This may include de-identified human medical data.

Public data is, of course, public, and has few restrictions.

So, the first step in developing a DSP is to describe the data that will be used in the research, and show which one of the three categories enumerated in Policy 5.10 that it belongs in. Then, describe how you will import the data from the external entity, and how you will store it while it is within Cornell, and how you will control and allow access to the data. A convenient tool to help find data storage solutions is: https://finder.research.cornell.edu/storage. And a more complete listing of regulated data and appropriate storage is found at: https://it.cornell.edu/regulated-data-chart. You can also find advice and help through the Research Data Management Group at Cornell: https://data.research.cornell.edu/services#Security,privacy,confidentiality

If there is a valid need to have the data stored on a local system, be it a desktop or a laptop, COECIS security procedures require that the local device be whole-disk encrypted and that the recovery key be escrowed with COECIS ITSG.

The next step is to demonstrate that the storage method and the research analysis process adequately control access to the data. For Cornell managed data storage, this usually means showing that only certain NetIDs or Active Directory groups will be allowed access to the data; this will ensure that the data will only be available to authorized users with valid individual passwords. If there is any local data storage, this requires a statement about the login access controls to the storage or analysis system, and any physical security.

Finally, the plan should acknowledge that the plan author (the PI or their designated proxy) are individual custodians of the data (as per Cornell policy 4.12, Data Stewardship and Custodianship) and will be responsible for controlling access to the data. https://www.dfa.cornell.edu/sites/default/files/policy/vol4_12.pdf

Also the plan should state the method of disposal or destruction of the data at the conclusion of the project.

COECIS ITSG staff can help you formulate a Data Security Plan, and the COECIS IT Security Director will have to approve the plan for submission to the IRB. You can submit your plan or request help by submitting an IT ticket at: https://help.coecis.cornell.edu

Click here to see a blank Data Security Outline

Data Security Plan Outline

1. What is the name of the project that the DSP applies to?

This Data Security Plan is for

1. What is the organization providing the data, and what is the name of the data set?
This research data will be obtained from

1. What are the specific data elements, and how are they generally formatted?

The data set is comprised of

1. How is this data classified, according to Cornell Policy 5.10?

Is this confidential data? (Y/N)______ Is this public data? (Y/N)______

Please explain any specific evaluations that you made to classify the data.

1. How will the data be transferred to Cornell?

The data will be transferred to Cornell by

1. Is there a Data Use Agreement or other document provided that has specific requirements affecting the use and storage of the data?

Is there a Data Use Agreement? (Y/N)______

Other:

1. Where and how will the data be stored?

Please describe where and how the data will be stored.
1. What are the access controls on the data storage method?

Describe the protections restricting and controlling access to the data.

1. Who will act as the project data custodian/custodians?

The project data custodians are

1. Are there backups of the data and/or data restoration procedures?

Describe any data backups and recovery procedures.

1. What will be the disposition of the data and copies at the close of the project?

Describe how you will handle the data and any copies or backups at the project completion.

1. Are there any other special considerations regarding the security of this data?

List and describe any special restrictions or required handling of this data, such as ITAR/EAR:
Spectre and Meltdown

For information on these vulnerabilities, please reference the following CIT Link: CIT Alert for Spectre and Meltdown

ITSG Staff are working with CIT on an action plan for Cornell Owned devices.