INTRODUCTION

The practices below can be used for ALL data collected or received by TC researchers. They are HIGHLY RECOMMENDED for sensitive data with identifiers. Research Projects that depart from or omit the procedures and resources below will need to provide a justification in the initial IRB application.

Computer and Information Services (CIS) offers support for TC-managed PCs and Macs. The initial point of contact should be the CIS Service Desk (servicedesk@tc.columbia.edu or x3300). The Service Desk can assist with the setup of all data access, collection, and storage resources that are outlined below. CIS does not support personal devices, but once these resources are configured, they can be accessed from personal devices.

DATA ACCESS

The primary investigator should designate roles and determine who has access to the research data. To ensure the integrity of research data, access to accounts and security of logins should be regularly reviewed (CIS recommends doing this at least every 6 months).

- Transmit data over a public or private network in safe and secure ways, such as a Virtual Private Network (VPN). TC’s Wifi network, as well as the networks at many data collection sites, are public, so for researchers anticipating using these networks, a VPN prevents data breaches. Contact the Service Desk to set up VPN access.

- Use only approved systems or tools to store, transmit, access and share data like TC Google drive, TC Dropbox, and TC DATA. TC Google Drive is already set up and available to all TC faculty and students as part of their Google suite. TC Dropbox accounts are only available to TC faculty, but access to these accounts can be assigned to students working on research projects once the TC Dropbox account has been set up. Contact the Service Desk to set up a TC Dropbox.

- Data administrators should ensure project staff are set up with unique user accounts and personal secret passwords. Project staff no longer involved in the project should have access removed immediately. The Service Desk can assist with removal of user accounts and provide tips on creating secure passwords.

- Regulate physical access to fixed and removable data-storage media and devices (e.g., hard drives, laptops, paper files, etc.). Data should be stored in a location with physical access by swipe card or keys controlled by the PI. Individual files on computers in shared offices should be encrypted.

- Avoid sharing any sensitive data through email and avoid using personal (non-TC) accounts for official Teachers College purposes.

- Don’t use USB flash drives to store or share data.
SECURE SYSTEM CONFIGURATION

All data deemed confidential or sensitive and stored on systems, accessed, shared or transmitted on the network must follow these standard guidelines.

- Configure systems with approved anti-virus/anti-spyware/anti-malware software by the Information Security Team (CIS).

- Encrypt backups with encryption keys only known to data owners or system administrators. The Service Desk can set up encryption for both Windows and Apple computers.

- Secure passwords and physical keys.

- Collect audit logs and develop alerts on anomalous behavior. Different systems have different means of doing this. The Service Desk can assist you with systems supported by TC.

SECURE DATA STORAGE

For storing data consider these recommendations.

- Use TC email and grant delegate access to staff to help ensure greater accountability and controls of access when students or staff members leave. Contact the Service Desk to set up delegate access.

- Use LastPass to share sensitive credentials to access any sensitive information. For more information on LastPass, please visit the CIS Website. The Service Desk can set up LastPass accounts for faculty and staff. Students can go to LastPass.com and download the free version of LastPass.

- Data of any kind should NOT be stored on USB thumb drives.

SECURE DATA COLLECTION

For secure data collection use these tools:

- Qualtrics – A web-based survey tool for creating and conducting online surveys.

- Redcap – A secure web application for building and managing online surveys and databases.

DO NOT USE Survey Monkey or other free web-based systems for collection of sensitive data. These systems are insecure and should only be used when collecting non-sensitive data.

DATA DISPOSAL

All confidential data, regardless of storage location, will be retained only as long as mandated by the third-party agreements, research project duration, legal, regulatory, business requirements, or other applicable standard. Please contact the Service Desk for guidance on proper disposal of data. Removable media such as tape media, optical discs (DVDs, CDs) and USB drives should not be used unless there is a clear justification.