**Additional security requirements for electronic and hardcopy data**

Describe the security procedures in place to safeguard electronic and/or hardcopy data. Even for anonymous data, there needs to be evidence that the researcher(s) have done their due diligence to protect the integrity of the data and/or datafile(s).

1. Which faculty and/or students will have access to the hardcopies and/or electronic data files that are created/used in this study?
2. If electronic data files are created/used, will the data be stored on a network, a local desktop or laptop computer, or an external data storage device (e.g. flash-drive)? Please specify.
3. If electronic data files are created/used—whether they’re stored on a computer, network, or external data storage device (e.g. flashdrive), access to the files on the computer, network, or external storage device holding the data files must be password-protected by a security login.
4. If electronic data files are created/used, who has access to the computers and/or data storage devices warehousing the data? This differs from question #1 in that it is specifically inquiring about access to office(s) that warehouse the computers or external data storage devices that hold the data.
5. Do the desktop and/or laptop computers used to access the data file(s) or store the data file(s) have an automatic log-out feature after a period of inactivity? If not, this protection must be activated to prevent unauthorized access to the data. Five minutes of inactivity is the standard time frame for when a computer should require re-entering a password.
6. Will the data be encrypted? This is not necessarily required, but it is recommended for sensitive data with any identifying information.
7. The data file(s) should not be emailed from one researcher to another, as this exposes the data file to possible interception from unauthorized parties. Instead, do an internal file transfer instead.
8. If you are using a web-based survey provider such as Survey Monkey, IP addresses should not be collected because this poses a threat to participants’ anonymity and confidentiality.