KU DEPARTMENT OF BIOSTATISTICS & DATA SCIENCE
The University of Kansas Medical Center

Shared Drive Usage Policy

When working with your mentor on your GRA assignment,

Things that can help a student efficiently complete their project's/tasks:

- Always store all the information and project related documents under the shared drive (S drive or P drive).
- During your first meeting with your mentor make sure a folder has been created and access is provisioned appropriately. For questions related to access, one could contact the Senior Data Scientist at spepper@kumc.edu and Director of Research Information Technology at dmudranthakam@kumc.edu
- For any reason, if you are working on data set and hasn't been assigned with a Department of Biostatistics & Data Science computer please check with either your mentor or Director of Research Information Technology.
- If you have any question or unsure as to how to handle the data or storage related issue please check with your mentor and/or the Seinor Data Scientist at spepper@kumc.edu and Director of Research Information Technology at dmudranthakam@kumc.edu .

you should **never**:

- Store documents containing sensitive information on laptop or notebook computers unless the computer is certified, and the information is encrypted. Call Information Security at ext. 8-3333 for information about personal computer certification and encrypting data.
- Store documents containing sensitive information on mobile devices such as iPhones or Personal Data Assistants (PDAs, Palms, PocketPCs, Windows CE devices, BlackBerries) unless such storage is approved by your department and the PDA is password-protected.
- Store sensitive information on small portable storage devices such as floppy drives, zip disks, flash memory drives (keychain drives, flash drives, USB memory keys), CDs, or DVDs unless the information is encrypted, and the device has been approved by Information Security.
- Store sensitive University information on a home computer or any other computer not owned by the University.

- Provide an outside entity with any type of sensitive information without the informed consent of your department chair. Be aggressive in seeking clarification and confirmation that including sensitive information is essential. While this may seem obvious in the case of (for example) patient information, it applies equally to a spreadsheet containing employee names and dates of birth or SSNs.
- Send any form of sensitive information off-campus via email using Outlook or any other email system except KUMC's Secure Email System. For information on the Secure Email System, please visit the secure email website.
- Post any form of sensitive information on a web server.
- Transmit files containing sensitive information outside of the KUMC network in a manner that does not utilize encryption to protect the communication (e.g., the SecureFiles system, SSL, VPN, etc).
- Store sensitive information in third-party online application services, unless a University contract with that vendor is in place which protects sensitive information.
- Store documents containing sensitive information on third-party online storage services, unless a University contract with that vendor is in place which protects sensitive information.

By providing my signature below, I confirm that I have read and agree to this document, and to not storing any type of data on personal devices.

_____ _____

Signature of Student Date

_____

Print Name of Student