Research Data Security Recommendations

- Update and patch hardware and software.
- Use encryption on your devices.
- Use Emory owned and managed devices.
- Minimize the use of personal devices as much as possible.
- A clean loaner laptop should be used for remote access.
- VPN must be used for remote access.
- When travelling offsite, maintain possession of your devices.
- Avoid travelling with data this isn't necessary.
- Register with International SOS before your trip.
- Know what types of data you are collecting, processing, storing, or sharing.
- Do not plug unknown peripherals into your Emory device.
- Do not download and save to desktop or a local drive.
- Know who has access to the data and apply appropriate access restrictions.
- Use SharePoint or OneDrive for data storage.
- Use strong passwords on devices and folders.
- De-identify data when possible.
- Have a data management plan.
- Securely destroy unneeded data.
- Report hacked, lost, or stolen devices as soon as possible to Emory Security

Rev3

For More Information, Contact:

researchsecurity@emory.edu
dataplans@emory.edu
ORAITHelp@emory.edu

EMORY UNIVERSITY | Research Compliance and Regulatory Affairs