#PrivacyAware

Tips for safeguarding data

- Know who has access to folders before you save restricted or critical data.
- Do not store sensitive data in locations that are publicly accessible from the Internet.
- Mobile or portable devices even for email use should be protected by a passcode and encrypted because they can be lost or stolen.
- Follow IU's passphrase requirements and NEVER share your pass phrase, use it for other services, or save it in memory!
- If sensitive data is no longer needed, don't retain it – follow your de partment's retention and disposal policies.
- Be on the lookout for phishing scams and forward suspicious email to phishing@iu.edu.
- Run anti-virus and anti-malware tools routinely and alert IT staff if you encounter issues.
- Do not use unencrypted wireless connections when working with or sending sensitive data. VPN and IUAnyWare are secure options.
- Do not send confidential data in an email unless the data is encrypted using slashtmp for critical data or CRES.
- For more information on protecting IU data, please visit https://protect.iu.edu/online-safety/protect-data/index.html

INDIANA UNIVERSITY
OFFICE OF THE EXECUTIVE VICE PRESIDENT FOR UNIVERSITY ACADEMIC AFFAIRS
University Public Safety