

KEEP DATA AT WORK *Secure*



01

VERIFY VERIFY VERIFY

Go above and beyond to verify ANY request to change bank info or contact details - no matter who the request comes from or who it is for (vendor, employee, partners, etc).

ENCRYPT SENSITIVE DATA

For sensitive information or data that is regulated, only use approved encrypted messaging tools and processes. NEVER keep sensitive data or passwords in a text file or spreadsheet.



02



03

GRAB THOSE DOCS ASAP!

Retrieve documents with sensitive information immediately and destroy them when no longer needed. Also, don't leave them lying around the office - keep them securely stored when not in use.

JUST SAY NO WHEN ON-THE-GO

It's easy to be distracted when working on-the-go via the mobile phone. Wait to deal with highly sensitive data when you're focused and alert on a secure work device.



04



05

AVOID PORTABLE DEVICES

Avoid putting personal or sensitive data on a portable device, such as a USB. Data should stay in an approved and protected location.

BACK IT UP!

Keep an offline backup of your data as a last resort in a - you guessed it - secure location.



06