Cybersecurity and Safety Recommendations

[Success by Design]

Best Practices Checklist

- ❑ Do not send unencrypted private data i.e. social security or account numbers via email.
- ❑ Do not text your advisor – texts are not archived and prohibited by regulatory agencies.
- ❑ Install and maintain a trusted anti-virus & malware protection program
- ❑ Store personal data on removable drives, then remove the drive when not needed.
- ❑ Do not utilize thumb drives from unknown sources
- ❑ Set strong passwords of at least 8 characters or more if possible
- ❑ Use different passwords for different accounts and change them at least yearly
- ❑ Utilize Dual Factor Authentication where available
- ❑ Do not store private data in Outlook, Excel, etc. (No credit cards, tax returns, healthcare data, etc.)
- ❑ Do not keep your credit cards and driver's license with your mobile phone case.
- ❑ Do not hand out or leave your house keys exposed, implement a keyless entry solution
- ❑ Do not open email attachments that you are not expecting, hover over links to reveal the actual URL.
- ❑ Be sure to keep your systems up-to-date on the latest software versions.
- ❑ Password protect devices when available