1. Recognize Phishing Attacks

- Phishing tries to get you to accidentally reveal confidential information, such as passwords or credit card numbers.
- Hover/focus over URLs before clicking links. If you don't recognize the site or it looks suspicious, don't click. Links and attachments in phishing emails can contain information-gathering malware. To do this on a mobile device, hold your finger down over the link and it will preview.

2. Reduce Physical Security Risks

- Always wear your badge on company premises and avoid wearing them in public places.
- Don't use your badge or credentials to grant access for others. They can always get a loaner badge from the reception desk.
- If you see someone without a badge, remind them to display it.
- Always check that your working environment is physically safe and protected.

3. Using Company Resources

- Only use your company email for work purposes. Don't send company data to non-company email addresses.
- Use company-managed computers only for business and limited personal use. Don't use company's intellectual property for personal use.
- Keep your work and personal devices' software up-to-date.

4. Protect Information and Data

- Don't print confidential documents unless absolutely necessary. Don’t share them with others if they don’t have a need to know. Use cross-cutting shredders to safely dispose of them at home or in the office.
- Wipe all writing boards after using the meeting rooms and remove or shred any printed documents.
- Don’t discuss confidential work topics in public places. Someone could overhear your conversation.
- Always lock your work computer when you step away - even at home.

5. Using Third-Party Applications or Services

- Download software only from approved company sources.
- Don't upload non-public company data to a third-party service or cloud.
- Get security approval for third-party services.

6. Handling Business Data

- Familiarize yourself with the different types of customer information and when to access it as defined by your company classification standards.
- It’s your responsibility to know what you can share outside of your company.
- Talk to your supervisor if you need more guidance in understanding what type of data you are working with, how to share, and store it securely.

7. Maintain Device Security

- Don't allow anyone else to use your company devices. Always store your company devices in a secure place out of sight when not using it.
- Unless absolutely necessary, don’t take your company devices with you when traveling, especially to high-risk areas.
- If your company device is lost or stolen, report it immediately to security.

8. Data Privacy - FERPA

- Be aware of data privacy. Data privacy involves the rights and obligations of individuals and organizations regarding the collection, use, retention, disclosure, and disposal of personal data. Personal data is information that can be linked, either directly or indirectly, to a particular person.
- If you process personal data, know the privacy risks. Processing of personal data includes collecting, retrieving, using, disclosing, sharing, and erasing personal data.

9. Safe Communication Habits

- Do not share private information.
- Keep security in mind with apps you use, who you send business information to, and what you share.

10. Recognize Social Engineering Threats

- Social engineers get you to react quickly rather than logically and they can be persuasive, convincing, and demanding. If you feel rushed or pressured, pause and think if someone is trying to get confidential information from you, or use your credentials to access information.
- Document as much information as possible about the incident (phone number, name, the website referenced) and report it to security.