CYBER HYGIENE: *Employee checklist*

ASANTE

All Asante employees and medical staff are responsible for practicing good cyber hygiene as a routine part of patient care. To make this simple, ITS Security has developed this checklist. It helps everyone stay clean of cyber security events and the damage they cause.

Treat Asante systems and data as if they were your own

- ✓ If it is electronic and used for Asante business and unprotected, don't wait for someone else to secure it.

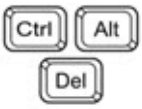
Be yourself

- ✓ Log into an Asante system only as yourself, not with a shared ID.
- ✓ Notify ITS if you are aware of systems that can be accessed via a shared ID so that a more secure login method may be implemented if possible.

Make passwords VERY hard to guess

- ✓ Cybercriminals can crack non-complex passwords in seconds or minutes.
- ✓ Using strong passwords with or without Duo is an absolute requirement for employees. Duo multifactor authentication is the most secure system-access method.

Ctrl Alt Delete before you leave your seat!



- ✓ Leave a blank or locked screen behind you when you get up.

Think before you click

- ✓ Assume all email is evil. Vet email before clicking on any links or opening any attachment.
- ✓ Help Asante by clicking the "Suspicious Email" or "Report a Phish" button visible on the email or Outlook controls ribbon whenever you think you may have a phish email.

Check before you connect

- ✓ If the electronic device is not owned or inventoried by ITS, it should not be connected to an Asante device or network without ITS approval.

Stay protected while connected

- ✓ Browse the Internet as if your mother or boss were watching.
- ✓ Avoid non-work-related sites (social media, entertainment, small retailers and political commentary, etc.), which are likely to draw phisherman and malware.

Don't download

- ✓ Don't take a chance. Downloading unexpected or untested software onto an Asante computer can have surprising consequences — including computer malfunction, infection and security breach. Always get ITS approval before downloading software to a company computer.

Spread the love: Engage our partners in cybersecurity

- ✓ Notice when non-employee, third-party vendors, contractors and business partners access Asante systems, whether on-site or remotely.
- ✓ Notify ITS if it appears that third-party security controls may be missing, unmonitored or remote open access to our systems and network.

If you see something, say something

- ✓ Take note that a critical piece of Asante's security defense is employee observations, questions, requests for help and reports of suspicious system or human activity.
- ✓ Immediately call the ITS Service Desk to report system or human suspicious activity or call us whenever you have cybersecurity questions or concerns.

To report an information security incident, call the ITS Service Desk at (541) 789-4141.