# Athens State University Cyber Security Campaign 2015

Employees play a critical role as the first line of defense in cybersecurity. Athens State University employees are urged to incorporate the following practices into their daily use of information and communication technologies at the University or away from work:

- Construct and use strong passwords; never use passwords that are easy to guess
- Do not leave computers unattended in public spaces
- Disable your computer by locking the keyboard or shutting down each time you leave your office
- Protect both institutional and personal data
- Read and understand the published security and privacy policies of the University
- Always think before clicking a web link
- Be cautious when dealing with all forms of electronic communication
- Do not fall prey to phishing attacks by responding to phone calls or e-mail requests for your account information (including password). Only you should initiate any communication about your account with the Help Desk
- Do not share personal identifiable information about employees or students - ever
- Protect mobile devices in the same manner as you do all desktop computers
- Report any suspicious e-mails, phones calls, or computer functions immediately to the Help Desk or your supervisor
- Promote cyber security awareness with colleagues and students
- Protect intellectual property rights, do not share copyrighted materials
- Promote and empower individuals by encouraging participation in cyber security training
- Practice safe computing at both work and home

At Athens State University, the following practices are already in place through the Information Technology Services implementation of Active Directory policies:

- Stay current on all operating system updates and patches
- Use antivirus and other safeguards to protect the desktop computer