Information Security

ISSO: 402-995-3858 or 402-995-3558

ALWAYS

• Lock your computer when out of eyesight of it. (Use the windows button + L, or go to the start menu and click “Lock”)
• Verify any requests for VA sensitive information before releasing it, even if the request seems harmless to you
• Use the access you’ve been given to the network only to perform your official duties. If you require more access, go through appropriate channels to get it.
• Use strong Passwords. Use a combination of uppercase and lowercase letters, numbers and symbols
• Treat your password like your toothbrush
  o Don’t share it
  o Change it regularly
  o Don’t leave it lying around
• Double Check mailings and faxes. Confirm the appropriate documents are being sent to the correct individual
• Report suspicious activity or security incidents. It is crucial that you report any suspicious activity or security incidents immediately to your supervisor, PO or ISSO (if you see something say something!)

NEVER

• Never share your password, PIV cards or other account information, even with trusted coworkers
• DO NOT plug phones into a VA computer to recharge them
• DO NOT send PHI/PII unencrypted
• Do not bring your personal removable media to the office
• You may NOT view your own Veteran records, nor that of your relatives, nor that of another employee, contractor or student Email is the only feature of Outlook where PII may be encrypted. Subject line of emails and calendar appointments, for example, may not contain PII. Skype is the instant messaging and screen share application. PII may be transmitted via Skype. SharePoint, like any website, if the address begins with https, then it may be considered secure. While PII may be placed on SharePoint, with the multitude of users, it is best not to put PII on SharePoint sites.