GPO

IT SECURITY AWARENESS PROGRAM FACT SHEET

GPO IT Security Policies:

- □ **GPO Directive 825.33B – IT Security Policy**
- □ **GPO Directive 825.29C – Internet & Email Use Policy**
- □ **GPO Directive 825.41A – Protection of Personally Identifiable Information (PII)**
- □ Passwords **Must**
- □ Be protected by users and changed every 60 days
- □ Be at least **8** characters long
- □ You **MUST** login to your computer every 30 days or your account will be disabled

- Passwords **Must Not**
  - Consist of dictionary words
  - Be shared with others OR stored in an insecure location
- Do not open or execute (double-click) Email attachments from unknown senders or unsolicited email
  - ➔ This is how many computer Viruses spread
- Do not click on web links contained in emails from unknown senders or unsolicited email
- Beware of clicking on web links in emails from any sender unless you were expecting an email from that person
- Do not connect non-GPO USB drives (flash drives, thumb drives, iPods, etc.) to GPO computers
- Do not connect GPO USB drives to non-GPO computers
- **Report IT security incidents to**
  - Your supervisor
  - IT Service Desk:

By Phone: Extension 202-512-1790

By Email: ITServiceDesk@gpo.gov

May 2019