

AAA-ICDR® Cybersecurity Checklist



-0	General Best Practice
	 □ Limit requests for and acceptance of sensitive information □ Avoid using free WiFi; use a personal hotspot instead □ Use a Virtual Private Network (VPN) service if using free WiFi cannot be avoided □ Report security incidents □ Take regular security awareness training □ Implement a document retention and destruction policy □ Back-up your critical data □ Buy cybersecurity insurance
— O	PC/Laptop/Mobile Devices
	 Lock PC, laptop and mobile devices with a password or pin Turn on full disc encryption on all devices Encrypt thumb drives (password required) and any other removable drives Use anti-virus software; update regularly Set-up and consistently accept automatic updates for PC, laptop and mobile devices Do not use PC/laptop administrative logon account for daily work; create a separate, limited-privilege account instead Turn on mobile device Wi-Fi only when needed Turn off Bluetooth when not in use Use a privacy screen
- O	Email Control of the
	 Avoid using free/personal email for case communications Don't email sensitive documents; use cloud storage or secure file transfer services instead Confirm sender before opening attachments or clicking on links
—	Password Hygiene
	 Use complex passwords or pass phrases Keep passwords private (do not write down or share) Use different passwords for different accounts; consider using a password manager Opt NOT to have your browser save passwords Use multi-factor authentication whenever offered for all your accounts