DKI APCSS Fellows Network
Rules of Behavior

These Rules of Behavior are applicable to the use of the DKI APCSS Information Technology (IT) services, devices and associated peripherals. The provided services and devices are to facilitate course activities only and the network should not be used for any other purposes.

DKI APCSS Fellows Kiosk v10.2022.0 Laptop

- Logout of all applications before leaving the DKI APCSS provided laptop unattended to prevent others from viewing or impersonating you when you are not around. The easiest method is to restart the computer.
- Do not attach any personal equipment to DKI APCSS provided laptop (e.g. external hard drives, USB flash/thumb drives).
- **The use of a wired headphone is authorized (e.g. 3.5mm or USB).**
- Never attempt to "test" or otherwise probe the security measures of the DKI APCSS network or provided laptop.
- Do **NOT** enter, copy, or otherwise process **ANY SENSITIVE DATA**.
- Access only data required to accomplish your course-related tasks.
- Protect your passwords. Do not reveal passwords to anyone. Notify the Seminar Leader if you suspect or know your account is compromised.
- Do not allow anyone to use your DKI APCSS provided laptop.
- Maintain accountability of your DKI APCSS provided laptop and associated peripherals at all times.

Internet Use While at the Center

- Only browse to sites associated with the completion of the course. Minimize all personal browsing.

Wireless BYOD Network Services

- Protect your wireless access username and password. Do not reveal passwords to anyone. Notify the Seminar Leader if you suspect or know your account is compromised.

Cyber Incident Reporting

- Immediately report all incidents of compromise, suspected compromise, unauthorized access (accidental or deliberate), disclosure of passwords, loss of equipment and related security violations to your Seminar Leader.

STANDARD MANDATORY NOTICE AND CONSENT PROVISION FOR ALL DOD INFORMATION SYSTEM USER AGREEMENTS

By signing this document, you acknowledge and consent that when you access Department of Defense (DoD) information systems:

1. You are accessing a US Government information system (which includes any device attached to this information system) that is provided for US government-authorized use only.
2. You consent to the following conditions:
   a. The US Government routinely intercepts and monitors communications on this information system for purposes including, but are not limited to, penetration testing, communications security monitoring, network operations and defense, personnel misconduct, law enforcement, and counterintelligence investigations.
   b. At any time, the US Government may inspect and seize data stored on this information system.
   c. Communications using, or data stored on, this information system are not private, are subject to routine monitoring, interception, and search and may be disclosed or used for any US Government-authorized purpose.
   d. This information system includes security measures (e.g., authentication and access controls) to protect US Government interests – not for your personal benefit or privacy.
   e. Notwithstanding the above, using an information system does not constitute consent to personnel misconduct, law enforcement, or counterintelligence investigative searching or monitoring of the content of privileged communications or data (including work product) that are related to personal representation or services by attorneys, psychotherapists, or clergy, and their assistants. Under these circumstances, such communications and work product are private and confidential, as further explained below:
      i. Nothing in this User Agreement shall be interpreted to limit the user's consent to, or in any other way restrict or affect, any US Government actions for purposes of network administration, operation, protection, or defense, or for communications security. This includes all communications and data on an information system, regardless of any applicable privilege or confidentiality.
      ii. The user consents to interception/capture and seizure of ALL communications and data for any authorized purpose (including personnel misconduct, law enforcement, or counterintelligence investigation). HOWEVER, consent to interception/capture or seizure of communications and data is not consent to the use of privileged communications or data for personnel misconduct, law enforcement, or counterintelligence investigation against any party and does not negate any applicable privilege or confidentiality that otherwise applies.
      iii. Whether any particular communication or data qualifies for the protection of a privilege, or is covered by a duty of confidentiality, is determined in accordance with established legal standards and DoD policy. Users are strongly encouraged to seek personal legal counsel on such matters prior to using an information system if the user intends to rely on the protections of a privilege or confidentiality.
      iv. Users should take reasonable steps to identify such communications or data that the user asserts are protected by any such privilege or confidentiality. However, the user's identification or assertion of a privilege or confidentiality is not sufficient to create such protection where none exists under established legal standards and DoD policy.
      v. A user's failure to take reasonable steps to identify such communications or data as privileged or confidential does not waive the privilege or confidentiality, if such protections otherwise exist under established legal standards and DoD policy. However, in such cases the US Government is authorized to take reasonable actions to identify such

communication or data as being subject to a privilege or confidentiality, and such actions do not negate any applicable privilege or confidentiality.

vi. These conditions preserve the confidentiality of the communication or data, and the legal protections regarding the use and disclosure of privileged information Further, the US Government shall take all reasonable measures to protect the content of captured/seized privileged communications and data to ensure they are appropriately protected.

f. In cases when the user has consented to content searching or monitoring of communications or data for personnel misconduct, law enforcement, or counterintelligence investigative searching, (i.e., for all communications and data other than privileged communications or data that are related to personal representation or services by attorneys, psychotherapists, or clergy, and their assistants), the US Government may, solely at its discretion and in accordance with DoD policy, elect to apply a privilege or other restriction on the US Government's otherwise-authorized use or disclosure of such information.

g. All of the above conditions apply regardless of whether the access or use of an information system includes the display of a Notice and Consent Banner. When a Banner is used, the Banner functions to remind the user of the conditions that are set forth in this User Agreement, regardless of whether the Banner describes these conditions in full detail or provides a summary of such conditions, and regardless of whether the banner expressly references this User Agreement.

- I understand that I may be held financially responsible for any computer equipment or associated peripherals that are not returned at the end of the course.
- I have read this document and understand my general responsibilities in the use and protection of DKI APCSS computer systems, network resources, and licensed software.
- I understand that failure to comply with the provisions of the established DKI APCSS Fellows Network Rules of Behavior may result in disciplinary action

Course: Course Name

Name: Full Name

Date: XX/XX/XXXX

Signature: *Full Name*