DKI APCSS Fellows Network
Rules of Behavior

The following Rules of Behavior are applicable to the use of the DKI APCSS Office 365 account, the Microsoft Surface Pro, and associated peripherals. The provided account and devices are to facilitate course activities. The network should not be used for any other purpose.

Microsoft Surface Pro

- Use only Asia Pacific Center for Security Studies (APCSS) AUTHORIZED SOFTWARE.
- Observe all software license agreements.
- Do not make unauthorized copies of software.
- Do not install or make changes to the software on the GFE.
- Log out or lock your system anytime you are going away from your terminal or computer. (Start ~Shutdown~ Logoff~OK or press the Windows and L key simultaneously, or hold ctrl-alt-del (simultaneously)~Lock Computer)
- Do not attach any personal equipment to the network (such as laptops and external hard drives). *The use of wired 3.5mm headphones are authorized.
- Use of USB flash/thumb drives is prohibited in Government Furnished Equipment (GFE).
- Never attempt to "test" or otherwise probe the security measures on the DKI-APCSS network or provided GFE.

Internet Use While at the Center

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

Microsoft Office 365 Account

- Microsoft Office 365 is hosted on DoD Impact Level 2 cloud environment. It is authorized to process public non-FOUO data or Non-Controlled Unclassified Information is data that is authorized for public release (i.e., , as well as some low confidentiality unclassified information NOT designated as Controlled Unclassified Information (CUI) or critical military/contingency operations mission data, but the information requires some minimal level of access control (e.g., user ID and password).
- Do not enter, copy, or otherwise process ANY CLASSIFIED OR SENSITIVE DATA.
- Access only data required to accomplish your course related tasks.
- Protect your Personal Authenticators (passwords). Do not reveal them to anyone. Notify the Computer Staff if you suspect or know your account has been compromised. Take special precautions when logging on to ensure that your Personal Authenticator is not disclosed to other personnel.
- Do not use another person's computer account or allow anyone to use your computer account.

Cyber Incident Report

- Report immediately all incidents of compromise, suspected compromise, unauthorized access (accidental or deliberate), disclosure of passwords, 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:

- You are accessing a U.S. Government information system (IS) (which includes any device attached to this information system) that is provided for U.S. government-authorized use only.
- You consent to the following conditions:
    - The U.S. Government routinely intercepts and monitors communications on this information system for purposes including, but are not limited to, penetration testing, communications security (COMSEC) monitoring, network operations and defense, personnel misconduct (PM), law enforcement (LE), and counterintelligence (CI) investigations.
    - At any time, the U.S. Government may inspect and seize data stored on this information system.
    - 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 U.S. Government-authorized purpose.
    - This information system includes security measures (e.g., authentication and access controls) to protect U.S. Government interests – not for your personal benefit or privacy.
    - 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:
        - Nothing in this User Agreement shall be interpreted to limit the user's consent to, or in any other way restrict or affect, any U.S. 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.
        - 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.

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

- 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 U.S. Government may, solely at its discretion and in accordance with DoD policy, elect to apply a privilege or other restriction on the U.S. Government's otherwise-authorized use or disclosure of such information.
- 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 ("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.

Course:

Name:

Date:

Signature: