AIR UNIVERSITY MICROSOFT 365 (AU M365) STATEMENT OF APPLICATION USE AND OF USER RESPONSIBILITIES

PART I

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 (USG) 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 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, and thus such communications and data are private and confidential. 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.

PART II

MANDATORY NOTICE & CONSENT FOR MICROSOFT 365 USER

- You will report to the proper authority within your respective organization any employee that you witness or who has witnessed someone conducting malicious activity while using this instance of Microsoft 365.

- If you are a government supervisor, you do not have the authority to access an employee's government-issued computer and /or device. The supervisor must receive approval from General Counsel for the Agency's Counter Intelligence Representative to review the employee's government-issued computer and or device.

- If you are a non-government supervisor, you must follow the legal guidelines of your agency with regards to accessing an employee's organization-issued computer and /or device.

- This application is intended for educational/public release information only. Neither U.S. Government or non-government organization owned information will be entered in or discussed on this application.

- 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.

PART III

AIR UNIVERSITY MICROSOFT 365 REQUIRED USER ACTIONS

- I will use AU M365 for educational collaboration/discussion only. I will not introduce or process data which the application has not been specifically authorized to handle. I may also be held both criminally/financially responsible for any damages that may occur to application or computing devices, if my actions are determined to be deliberate, willful, or malicious.

- I understand the need to protect all passwords. I will not share my license, password(s) or account (s) information with coworkers or personnel not authorized to access the application.

- I am responsible to check the validity of the Microsoft 365 Web sites prior to signing on by reviewing the digital certificates on the site to ensure they are issued/signed by Microsoft and show no certificate errors.

- I am responsible for configuring my browser to use the recommend encryption level by enforcing the use of TLS encryption through the security menu of the browser.

- I am responsible for ensuring my device and browser are properly updated with most recent vendor patches.

- I am responsible for all actions taken under my account(s). I will not attempt to "hack" the application or gain access to data which I am not authorized to access.

- I understand I must complete designated IA training before receiving system access.

PART IV

AIR UNIVERSITY MICROSOFT 365 PROHIBITED USER ACTIVITIES

- Introducing classified or controlled unclassified information (FOUO, LES, DoD UCNI, and Limited Distribution) belonging to the U.S. Government, my organization, or containing Privacy Act (personally identifiable/personal health information) or other protected personal information.

- Accessing, storing, processing, displaying, distributing, transmitting, or viewing material that is abusive, harassing, defamatory, vulgar, pornographic, profane, racist, promotes hate crimes, or subversive in nature, or objectionable by nature to include; material that encourages criminal activity or violates any applicable local, state, Federal, national, or international law.

- Creating, processing, storing, or transmitting entertainment media or other files not related to the objectives of AU M365. This includes freeware, shareware, copyrighted commercial and non-commercial software, and all other forms of software and files not directly related to the educational and administrative purposes of AU M365.

- Knowingly writing, coding, compiling, storing, transmitting, or transferring malicious software code, to include viruses, logic bombs, worms, and macro viruses.

- Engaging in prohibited political activity.

- Using the application for personal financial gain such as advertising or solicitation of services, sale of personal property, or stock trading (i.e., issuing buy, hold and/or sell directions to an online broker).

- Engaging in fundraising activities, either for profit or non-profit.

- Gambling, wagering, or placing of any bets.

- Writing, forwarding, or participating in chain letters.

ALL MUST READ AND SIGN:

I will immediately report any person suspected of engaging in, or any other indication of, computer network intrusion unexplained degradation or interruption of application services, or the actual or possible compromise of data or file access controls to the appropriate Cyber Security (formerly IA) management or team representatives.

I agree to notify the organization that issued the account when access is no longer required.

I understand that failure to comply with the requirements of this User Agreement will be reported and investigated. The results of the investigation may result in one or all of the following actions:

- Immediate revocation of application access and/or user privileges
- Job counseling, admonishment
- Revocation of Security Clearance
- Uniform Code of Military Justice and/or criminal prosecution
- Disciplinary action, reassignment, discharge, or loss of employment

I HAVE READ AND UNDERSTAND THE REQUIREMENTS AND WILL COMPLY WITH THE REQUIREMENTS SET FORTH IN THIS AGREEMENT. IN THE EVENT OF CONFLICT, PART I TAKES PRECEDENCE OVER PART II ABOVE.

Signature: _____ Printed Name: _____

Organization: _____ Date: _____

DIGITAL SIGNATURE IS ACCEPTABLE IF ABLE TO PROVIDE: