



DEPARTMENT OF DEFENSE  
NATIONAL DEFENSE UNIVERSITY  
WASHINGTON DC 20319-5066

MEMORANDUM FOR ALL PERSONNEL

APR 13 2018

SUBJECT: Data Usage Guidance

References:

- (a) 5 U.S.C. 552a, Privacy Act of 1974
- (b) CJCSM Instruction 6510.01F, "Information Assurance and Cyber Network Defense," June 9, 2015
- (c) DoDI 5200.01, "DoD Information Security Program and Protection of Sensitive Compartmented Information (SCI)," April 21, 2016
- (d) DoDD 5400.11, "Department of Defense Privacy Program," October 29, 2014
- (e) DoD 5500.07-R, "The Joint Ethics Regulation," March 25, 1996
- (f) DoDI 8500.01, "Cybersecurity," March 14, 2014
- (g) DoDI 8510.01, "Risk Management Framework (RMF) for DoD Information Technology (IT)," March 12, 2014
- (h) Executive Order 13556, "Controlled Unclassified Information," November 4, 2010
- (i) National Defense University (NDU), "NDU Governance and Privacy Policy (AR-1)," June 8, 2017
- (j) National Defense University (NDU), "NDU Security Awareness and Training Policy (AT-1)," June 29, 2017
- (k) National Defense University (NDU), "NDU System Access Authorization Request (SAAR) Form 2875," January 5, 2018
- (l) National Institute for Standards and Technology, Special Publication 800-53 Revision 4 with updates, "Security and Privacy Controls for Federal Information Systems and Organizations," January 22, 2015
- (m) Rehabilitation Act of 1973, Section 508 Amendment

Releasability: Cleared for public release.

1. Applicability: In compliance with requirements set forth in References (a) through (m), this memorandum provides specific guidance for all NDU faculty, staff, personnel and students who use any NDU information technology resource for processing, storing, displaying, communicating or researching.

2. Non-NDU Based Data Systems (Cloud Storage): Cloud Storage systems include any application, mobile or browser based, that is hosted by a third party through the Internet and outside the NDU and DoD network boundaries. Applications such as Blackboard and Microsoft Office365 are examples of cloud systems. The following data are PROHIBITED IN CLOUD STORAGE SYSTEMS:

- a. Personally Identifiable Information (PII) as defined in Reference (d).

Exceptions: Per DoD CIO instruction: faculty, staff and student work email, work phone numbers and other Government or Corporate data are not considered PII and are allowable.

- b. Controlled Unclassified Information (CUI) in accordance with Reference (h).
- c. Any data not directly related to programs and functions supporting the approved NDU mission statement.
- d. Personal data not in compliance with References (e) and (k).
- e. Data not directly related to academic instructional or research programs provided at NDU.
- f. Any course content that is not Section 508 compliant (Reference (m)).
- g. Data files that exceed 10 MB. Judicious selection and compression of high quality learning assets is required.

3. On-premises systems include all applications and data storage that reside inside the NDU networks. Examples include Microsoft Office (desktop versions), and university shared drives for file storage. The following data are PROHIBITED IN ON-PREMISES SYSTEMS:

a. Personally Identifiable Information (PII) and other Controlled Unclassified Information (CUI) that are not encrypted and stored in accordance with the NDU Governance and Privacy Program Policy and Procedures (AR-1) (Reference (i)) and other DoD guidance.

Exceptions: Per DoD CIO instruction, faculty, staff and student work email, work phone numbers and other Government or Corporate data are not considered PII and are allowable.

- b. Any data not directly related to instructional or research programs and functions supporting the approved NDU mission statement.
- c. Personal data not in compliance with References (e) and (k).
- d. Any course content that is not Section 508 compliant (Reference (m)).
- e. Data files that exceed 10 MB. Judicious selection and compression of high quality learning assets is required.

4. All data currently stored in any NDU systems that are in violation of DoD and NDU data policy shall be electronically deleted from the system by the owner.

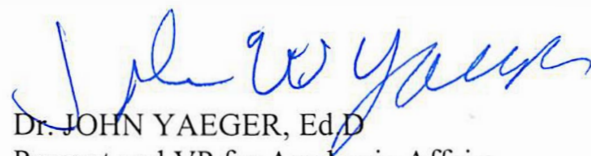
a. Account holders are ultimately responsible to manage their own data and should periodically perform a self-check and immediately purge any data not compliant with the guidelines.

b. If any NDU account holder is in receipt of data prohibited by NDU policies, the receiving user is responsible for removing the information from the NDU environment and notifying the sender to cease transmitting.

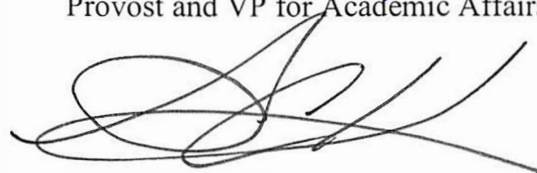
c. ITD will periodically review NDU systems for well-known non-compliance issues and an ITD POC will provide notification to individuals who are not compliant within three (3) working days.

d. If any identified data compliance issue is a “false positive,” meaning that an automated tool or manual review has identified a file as being non-compliant when in fact it is compliant, the user must provide explanation to the ITD POC that contacted them within three (3) days of the notification as verified by email receipt.

5. For questions about NDU's technology and computing environment, please contact the ITD Service Desk at 202-685-3824.



Dr. JOHN YAEGER, Ed.D  
Provost and VP for Academic Affairs



ROBERT KANE  
Chief Operating Officer

CF:  
CIO Cybersecurity Team