



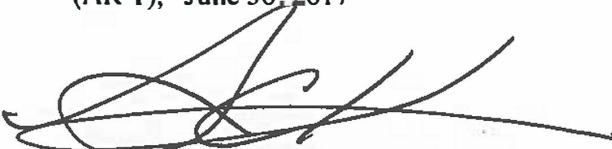
NDU INSTRUCTION 8500.02 GOVERNANCE AND PRIVACY PROGRAM POLICY AND PROCEDURES (AR-1)

Originating Component: Information Technology Directorate, ITD

Effective: July 6, 2018

Releasability: Cleared for public release. Available on the NDU Intranet at <https://portal.ndu.edu/Pages/Home.aspx>.

Incorporates and cancels: "NDU Governance and Privacy Program Policy and Procedures (AR-1)," June 30, 2017

Approved by: 
Robert Kane, Chief Operating Officer

Purpose: In accordance with the National Defense University (NDU) Cybersecurity Program catalog of the Baseline Cybersecurity Requirements (BLCRs) for all NDU information technology (IT) resources, this document presents the NDU policy and procedures to comply with applicable privacy protection requirements and minimize overall privacy risk.

The Risk Management Framework contains several control families that address multiple facets of privacy information management. All appropriate control families related to privacy are centralized and addressed together in this document. The control families include:

- AP Authority and Purpose
- AR Accountability, Audit, and Risk Management
- DI Data Quality and Integrity
- DM Data Minimization and Retention
- IP Individual Participation and Redress
- SE Security
- TR Transparency
- UL Use Limitation

TABLE OF CONTENTS

SECTION 1: GENERAL PROCEDURE INFORMATION.....	3
1.1. Applicability.....	3
1.2. Policy.....	3
1.3. Background.	3
SECTION 2: ROLES AND RESPONSIBILITIES.....	5
2.1. Chief Information Officer (CIO).	5
2.2. Chief Information Security Officer (CISO).....	5
2.3. Chief Operating Officer (COO).....	5
2.4. Component Privacy Officer (SCOP).	5
2.5. Chief Program Management Division (PMD).....	5
2.6. Records Manager (RM).....	5
2.7. System Administrator/Developer (Network, Database, and Server Engineers).	5
2.8. System Owner (SO).....	5
SECTION 3: PROCEDURES.....	6
3.1. Privacy Plan.....	6
3.2. Authority and Purpose (AP).....	6
3.3. Accountability, Audit, and Risk Management (AR).	7
3.4. Data Quality and Integrity (DI).	11
3.5. Data Minimization and Retention (DM).	12
3.6. Individual Participation and Redress (IP).....	15
3.7 Security (SE).	18
3.8. Transparency (TR).	21
3.9 Use Limitation (UL).....	23
GLOSSARY	24
G.1. Acronyms.	24
G.2. Definitions.	24
REFERENCES.....	26
APPENDIX A: SAMPLE PRIVACY STATEMENT FOR SYSTEMS.....	28
APPENDIX B: SAMPLE PRIVACY STATEMENT FOR FORMS.	29
APPENDIX C: SAMPLE TERMS OF USE FOR NDU APPLICATIONS.....	30
APPENDIX D: DOCUMENT CONTROL TABLE.....	31

SECTION 1: GENERAL PROCEDURE INFORMATION

1.1. APPLICABILITY. Applicable to all NDU colleges and components, employees and contractors.

1.2. POLICY. It is NDU's policy that the Governance and Privacy procedures herein:

a. Establish the required security controls to provide guidance and procedures for the implementation and management of the NDU Privacy Program.

b. Must be followed for all NDU systems. System Owners must ensure that all privacy policies and procedures are followed on each individual system, and controls that are system-specific must be included and properly documented in the appropriate system documentation.

1.3. BACKGROUND.

a. Purpose of Privacy Information at NDU. Because students are at the core of NDU's mission, PII constitutes a significant part of the data needed to make the mission. NDU collects and stores this data primarily to facilitate the student lifecycle and other major processes. The Department of Defense, in congruence with the rest of the Federal Government, employs the following definition of PII in DoD 5400.11, DoD Privacy Program (Reference (g)):

Information used to distinguish or trace an individual's identity, such as name, social security number, date and place of birth, mother's maiden name, biometric records, home phone numbers, other demographic, personnel, medical, and financial information. PII includes any information that is linked or linkable to a specified individual, alone, or when combined with other personal or identifying information.

b. Information Types. The types of personal information collected in the NDU systems hosted on the NDU Enterprise Information System (NEIS) include an individual's name, address, e-mail address, phone number, sex, age, social security number, marital status, education, attributes pertaining to US and Foreign military, civilian, and inter-agency personnel, records related to student course enrollments and final grades. This data is critical to generate official transcripts for students, Program for Accreditation of Joint Education (PAJE) reports, and Middle States accreditation reports. It is also used to facilitate travel and logistics for foreign nationals who attend the university, as well as HR actions for military students. A combination of military, civilian, and/or contract personnel access different combinations of this data in several IT systems.

c. PII for International Students. NDU hosts a number of international students and/or fellows each year, and the rules for PII are slightly different for foreign national students. NIST Special Publication 800-122, "Guide to Protecting the Confidentiality of PII," (Reference (t)) notes the term "individual" is defined as a citizen of the United States or an alien lawfully admitted for permanent residence. However, this guidance allows organizations to choose to administratively expand the scope of application to foreign nationals – and in some cases, such expansion is required by other laws and treaties. For example, the Immigration and Nationality Act requires the protection

of the confidentiality of Visa applicant data, which is not explicitly covered in DoD 5400.11 (Reference (g)).

SECTION 2: ROLES AND RESPONSIBILITIES

2.1. CHIEF INFORMATION OFFICER (CIO). Approve or prohibit technologies or services for all NDU systems.

2.2. CHIEF INFORMATION SECURITY OFFICER (CISO). Oversees the establishment and maintenance of a security operation that, through automated and continuous monitoring, can detect, contain and mitigate incidents that impair information security and agency information systems. Develops, maintains and oversees the NDU Cybersecurity Program.

2.3. CHIEF OPERATING OFFICER (COO). Appoints the Component Privacy Officer.

2.4. CHIEF PROGRAM MANAGEMENT DIVISION (PMD). Works with the CIO and ITD Senior Leadership to allocate resources for the Privacy Program.

2.5. RECORDS MANAGER (RM). Works with the CIO and other University personnel to ensure that privacy information is identified in official records and archived according to the National Archives and Records Administration (NARA) Records Management schedule.

2.6. SENIOR COMPONENT OFFICIAL FOR PRIVACY (SCOP). Has agency-wide accountability for NDU's privacy program.

2.7. SYSTEM ADMINISTRATOR/DEVELOPER (NETWORK, DATABASE, AND SERVER ENGINEERS). Ensures that secure configuration settings are built into applications or systems in accordance with security requirements and assists with security impact analyses and configuration monitoring activities as needed. In addition, may be included in the process for determining the appropriate baseline configuration for relevant configuration items (CIs) and may serve on configuration boards. Also responsible for complying with Cybersecurity policies and implementing Cybersecurity procedures.

2.8. SYSTEM OWNER (SO). Responsible to maintain a baseline and control over their information system's configurations and documentation throughout the system's lifecycle for the overall procurement, development, integration, modification, operation, maintenance, and disposal of that system.

SECTION 3: PROCEDURES

3.1. PRIVACY PLAN. The SCOP oversees the Privacy Plan provisions herein to implement all applicable privacy controls, policies and procedures.

a. Privacy Plan Updates. The SCOP ensures that the Privacy Plan, policy, and procedures are updated biennially (every two years). This document constitutes the NDU Privacy Plan. This activity entails:

(1) Working with the NDU ITD Operations team to check the inventory of NDU Systems to ensure that all systems that gather PII have an appropriate system notification/warning banner about Privacy. See Appendix A for sample wording.

(2) Coordinating with the NDU Forms Custodian and the NDU Chief Operating Officer to check the inventory of NDU Forms to ensure all forms that gather PII (paper or electronic) contain a privacy statement in accordance with (IAW) Reference (g). See Appendix B for sample wording.

(3) Disseminating this document and all subsequent updates by:

(a) Posting after each update on the NDU SharePoint Policy Repository page

(b) Disseminating directly to all personnel listed in Section 2: Roles and Responsibilities.

3.2. AUTHORITY AND PURPOSE (AP).

a. Authority to Collect (AP-1). The SCOP determines and documents the legal authority that permits the collection, use, maintenance, and sharing of PII, either generally or in support of a specific program or Information System need. The authority for NDU to collect PII is detailed in 10 U.S.C. 2165, National Defense University; 10 U.S.C. 2163 Degree Granting Authority for National Defense University and E.O. 9397, as amended (SSN).

b. Purpose Specification (AP-2). The SCOP ensures that all appropriate NDU entities describe the purpose(s) for which PII is collected, used, maintained, and shared in its privacy notices. The Purpose Specification will generally read:

The data provided will be used to update your National Defense University (NDU) record. NDU data are used to authenticate and identify NDU personnel and students; track academic enrollment, assignments, progress, and assessments; track personnel records and actions; create academic transcripts and related reports; facilitate award of degrees and credentials; conduct analysis for regional and DoD academic accreditations; and create reports for University leadership to aid in the development of effective curricula.

3.3. ACCOUNTABILITY, AUDIT, AND RISK MANAGEMENT (AR). The CIO develops, disseminates, and implements operational privacy policies and procedures that govern the appropriate privacy and security controls for programs, Information Systems, or technologies involving PII. This information is disseminated on the NDU Intranet in SharePoint [at this link](#) so that it is accessible to all NDU personnel.

a. Governance and Privacy Program (AR-1).

(1) Component Privacy Officer Appointment. The Senior Agency Official for Privacy (SAOP) is appointed at the DoD Chief Management Officer (CMO) level. NDU falls under the Joint Staff, which falls under Office of the Secretary of Defense (OSD) Privacy Office. The NDU COO appoints a Component Senior Official for Privacy (SCOP) accountable for developing, implementing, and maintaining an organization-wide governance and privacy program to ensure compliance with all applicable laws and regulations regarding the collection, use, maintenance, sharing, and disposal of PII by programs and Information Systems. If deemed necessary, an Assistant Privacy Officer may also be appointed at the discretion of the COO. The Assistant Privacy Officer shall serve as Acting NDU Privacy Officer when the Component Privacy Officer is otherwise unable to perform the functions and duties of the office. The SCOP relationships and duties are specified in the Appointment Letter for the position.

(2) Monitoring Privacy Laws and Policy. The SCOP monitors federal privacy laws and policy for changes that affect the privacy program. Additional information about how NDU maintains currency with privacy laws and policy is referenced in ITD document PM-15, Contact with Security Groups and Associations (Reference (1)). This monitoring is accomplished at NDU in the following forms:

(a) SCOP general awareness of all legislation, Executive Orders, Office of Personnel Management, and any other Government entity or instrument having governance over privacy information

(b) Cybersecurity Team participating in Cybersecurity continuing education courses

(c) PO, NDU Security and ITD Cybersecurity team members' attendance at CIO, DoD and Government Cybersecurity forums and programs

(d) Information disseminated by Army Research Lab (ARL) and Defense Information Systems Agency (DISA)

(3) Budget Allocation for Privacy Program. The COO works with the NDU Budget Officer and the ITD Chief, Program Management Division, to ensure the allocation of sufficient resources, staffing and budget to implement and operate the NDU-wide privacy program. The Privacy Program is accounted for in the overall resources required for the Cybersecurity Team. The Chief Information Security Officer (CISO) provides data and analysis to the CIO and Chief PMD annually to ensure the budget allocations are realistic. The NDU ITD Information Security Workforce Plan (PM-13) provides more information about the process to provide resource inputs into the budget.

b. Privacy Impact and Risk Assessment (AR-2).

(1) The CISO, with input from the SCOP, documents and implements a privacy risk management process and documents identified risks in accordance with NDU Risk Management Strategy (PM-9) (Reference (r)). The SCOP is responsible for monitoring all Government guidance related to privacy and recommending updates to the NDU Risk Management Strategy (see section 3.3.1.2).

(2) The CISO has documented an overall NDU Privacy Impact Assessment (PIA) for NDU and provided the PIA to the Authorizing Official (AO). The CISO will update this assessment as required or requested by the AO to maintain Authority to Operate (ATO) for all NDU IT Infrastructure and major IT systems. The official copy of the PIA is kept up-to-date in eMASS and in ITD's Cybersecurity information repository.

(3) For specific systems, a complete assessment of privacy risk to individuals resulting from the collection, sharing, storing, transmitting, use, and disposal of PII is required. The System Owner documents the assessment by completing the DoD Standard Privacy Impact Assessment Form, DD Form 2930 (Reference (e)).

(4) The CISO shall require, and review, PIAs for all Information Systems as part of the normal ITD Configuration Management Policy and Procedures (CM-1), prior to deployment or major update of any system. The PIA is submitted to the Authorizing Official for the system. A copy of the PIA shall be maintained as part of the official record of the system in ITD's Cybersecurity information repository.

(5) Outside the scope of IT Systems, the SCOP will maintain awareness of programs, and any other manual collection methods such as forms or other activities, that pose a privacy risk in accordance with applicable law, Office of Management and Budget (OMB) policy, or any existing organizational policies and procedures. The SCOP will document risks and provide them immediately upon discovery to the CISO so that they may be tracked in accordance with the NDU Risk Management Strategy.

c. Privacy Requirements for Contractors and Service Providers (AR-3). Contractual requirements related to privacy, to include privacy roles, responsibilities, and access requirements, are documented in the contract and/or other acquisition related documents for each contractors and/or service provider. Access to privacy information is based on need to know, in other words, the access is required in order to meet the objectives put forth in the contract. The SCOP serves as a resource to the NDU Resource Management Division and the ITD Chief, Program Management Division, to provide appropriate language to include in privacy management and information handling requirements within contracts and other acquisition-related documents. Privacy requirements shall be included in contracts in accordance with privacy requirements from Federal Acquisition Regulation Subpart 24.1, 48 CFR Part 24 and Part 39.105, and DoDD 5400.11 (Reference (g)).

d. Privacy Monitoring and Auditing (AR-4). Privacy controls and internal privacy policy are audited every three years, or whenever there is a major system change involving privacy

information. Audits are performed in accordance with the NDU accreditation cycle. The following describes the audit procedures:

(1) The controls outlined in this policy and procedure document serve as the framework for the audit criteria.

(2) IAW the Privacy Program Schedule, the SCOP or designee reviews each control and checks for current evidence. If necessary, copies of evidence are made for the audit.

(3) All privacy controls and their implementation status are recorded in a spreadsheet or database tool. Outstanding privacy controls not yet compliant are recorded in NDU's POA&M which is maintained in the eMASS system.

(4) eMASS serves as the record of the audit. The SCOP conducts interim reviews annually on a minimum of 1/3 of the privacy controls in this document to ensure their requirements are consistently met.

e. Privacy Awareness and Training (AR-5). The SCOP and CISO develop, implement, and update a comprehensive training and awareness strategy aimed at ensuring that personnel understand privacy responsibilities and procedures. This is accomplished at NDU by:

(1) Administering basic privacy training annually. Upon account creation and annually thereafter, all NDU employees (faculty and staff), as well as all contractors with computer access, complete "Joint Staff Annual Privacy Act Training and Safeguarding PII" available through Joint Knowledge Online. All personnel must present the required training certificate before receiving access to any electronic NDU resource, and annually thereafter. Details about the training may be found in the NDU Security Awareness and Training Policy and Procedures (AT-1) and course information is found in the NDU Threat Awareness Program (PM-16).

(2) Targeted, role-based privacy training for personnel having responsibility for PII or for activities that involve PII annually.

(3) The SCOP or designee shall check for annual training compliance. Personnel who have access to NDU electronic resources and do not renew their required privacy training annually shall have their account access removed until the training requirement is complete.

(4) All personnel shall indicate on the NDU 2875 that they accept responsibility for privacy requirements.

f. Privacy Reporting (AR-6). The SCOP develops, disseminates, and updates reports to oversight bodies, as appropriate, to demonstrate accountability with specific statutory and regulatory privacy program mandates as well as provide needed data for external reports. As they are created, the SCOP also provides reported information to NDU senior leadership, the CISO, and other personnel with responsibility for monitoring privacy program progress and compliance. Annually or as requested, the SCOP will summarize key findings for NDU leadership to inform improvements or changes to the Privacy Program. Reporting requirements include inputs to:

(1) Annual report of incidents involving privacy information to Washington Headquarters Services (WHS) Records Privacy and Declassification Division

(2) Federal Information Security Management Act (FISMA) Section D (privacy) reports to WHS Records Privacy and Declassification Division

(3) Section 803 Privacy and Civil Liberties bi-annual report to WHS Records Privacy and Declassification Division

(4) DoD Director of Administration and Management (DA&M) and/or the OCIO to support reports to OMB

(5) Congress and other oversight bodies

g. Privacy-Enhanced System Design and Development (AR-7).

(1) The CISO, through the ITD Configuration Management Policy and Procedure (CM-1), is responsible for reviewing all systems before deployment and on major updates, to ensure all Information Systems appropriately support privacy by automating privacy controls where possible. The definition of what constitutes “appropriate” controls must be supported by, and align with, the documentation of the system’s PIA. This may be documented aCCI-003456long with the Security Impact Analysis (SIA) for the system. The NDU ITD Requirements Vetting and PMO Process (Reference (n)) illustrates where in the development process the SIA must be completed.

(2) To the extent possible and where resources and budget allow, NDU will employ automated methods such as Data Loss Prevention (DLP) and other automated policies and rules to protect privacy information. While such automation provides additional layers of protection, these methods do not negate the personal responsibility of all NDU faculty, staff and students for safeguarding privacy information.

h. Accounting of Disclosures (AR-8). As a general practice, NDU does not disclose privacy information except through official Government channels and only as specifically needed to facilitate a person’s transfer of official Government records, for example, to and from a student’s home agency. Any other requests for NDU’s institutional data are handled through the Director of Institutional Research, who:

(1) Keeps an accurate accounting of disclosures of information held in each system of records under its control (in the form of an auditable log), including:

(a) Date, nature, and purpose of each disclosure of a record

(b) Name and address of the person or agency to which the disclosure was made

(2) Retains the accounting of disclosures log for the life of the record or five years after the disclosure is made, whichever is longer (refer to NDU Records Management Policy)

(3) Makes the accounting of disclosures available to the person named in the record upon request

i. Disposal of PII.

(1) Federal records must be disposed of in accordance with the approved National Archives and Records Administration (NARA) retention and disposal schedule, in accordance with NDU Records Management policy (Reference (s)).

(2) After contacting the NDU RM to ensure NARA compliance, NDU personnel who need to dispose of paper or electronic records containing PII may use any means that prevents inadvertent compromise. A disposal method is considered adequate if it renders the information unrecognizable or beyond reconstruction. Disposal methods may include:

- (a) Burning
- (b) Melting
- (c) Chemical decomposition
- (d) Pulping
- (e) Pulverizing
- (f) Shredding
- (g) Mutilation
- (h) Degaussing
- (i) Delete/Empty Recycle Bin

3.4. DATA QUALITY AND INTEGRITY (DI). DI controls ensure that any PII collected and maintained by organizations is accurate, relevant, timely, and complete for the purpose for which it is to be used.

a. Data Quality (DI-1). Guidelines ensuring and maximizing the quality, utility, objectivity, and integrity of disseminated information are consistent with DoD 5400.11-R (Reference (h)) and include:

(1) Ensuring and Maximizing Data Quality: the NDU Enterprise Information Architecture (Reference (m)) includes standards for authoritative data sources and formats to be used for all university records.

(a) All systems confirm to the greatest extent practicable upon collection or creation of PII, the accuracy, relevance, timeliness, and completeness of that information; this confirmation is done through automated validation of formats, data integrity checks, confirmation pages, and other

automated methods. In addition, all systems collect PII directly from the individual to the greatest extent practicable

(b) The Registrars for each component validate the personal information of NDU students throughout the student lifecycle, including: upon application, enrollment, registration, and graduation/completion of programs. Registrars must designate quality assurance methods to check for, and correct as necessary, any inaccurate or outdated PII used by programs or systems annually.

(c) PII quality assurance guidelines must be followed in accordance with DoD 5400.11-R (Reference (h)) to ensure accuracy, relevance, timeliness, and completion of PII prior to its dissemination.

(2) Data Utility: PII may only be used for NDU official business and the usage of PII shall be minimized to the greatest extent possible. Sharing of PII must be specifically authorized by the NDU Registrar.”

(3) Data Objectivity: No PII may be used at NDU to make decisions about benefits or services received from the University.

(4) Data Integrity: NDU data sources are implemented with data integrity checks (such as foreign keys, lookup tables and other standard data tools) to ensure correctness and consistency of records. The NDU Enterprise Information Architecture (Reference (m)) contains authoritative lists that can be used for data integrity checks.

b. Validate PII (DI-1 (1)). The System Owners ensure that all systems, when collecting PII, request that the individual (or individual’s authorized representative) validate PII during the collection process. This includes giving the user providing the information a chance to confirm all entered information is correct, and if it is not, gives the user an opportunity to provide and save corrections.

c. Re-Validate PII (DI-1 (2)). The Registrars for each component validate the personal information of NDU students throughout the student lifecycle, including: upon application, enrollment, registration, and graduation/completion of programs.

d. Data Integrity and Data Integrity Board (DI-2). A computer matching program is required pursuant to the Privacy Act of 1974 for any computerized comparison of two or more automated systems of records, or a system of records with non-federal records, for the purpose of establishing or verifying eligibility or compliance as it relates to cash or in-kind assistance or payments under federal benefit programs. NDU does not participate in Computer Matching Agreements, so this control does not apply.

e. Publish Agreements on Website (DI-2 (1)). NDU does not participate in Computer Matching Agreements, so this control does not apply.

3.5. DATA MINIMIZATION AND RETENTION (DM). The Data Minimization and Retention (DM) controls in this section ensure data minimization and retention requirements to collect, use, and retain only PII that is relevant and necessary for the purpose for which it was originally

collected. NDU retains PII for only as long as necessary to fulfill the purpose(s) specified in public notices and in accordance with a National Archives and Records Administration (NARA)-approved record retention schedule. Then the information is disposed of, in accordance with the section of this policy titled “Data Retention and Disposal (DM -2).”

a. Minimization of PII (DM-1).

(1) NDU has identified the minimum PII elements that are relevant and necessary to accomplish the legally authorized purpose of collection. These data elements are documented in the NDU Enterprise Information Architecture and published in the NDU System of Records Notices (SORNs). The data elements are also listed in this document in the section titled “Locate / Remove / Redact / Anonymize PII (DM-1 (1)).”

(2) NDU limits the collection and retention of PII to the minimum elements identified for the purposes described in the SORN and for which the individual has provided consent. Unique PII elements such as Social Security Number, Taxpayer Identification Number, Foreign Identification Number, or any other unique identifier that did not originate at NDU, should never be stored or transmitted outside a mechanism that is encrypted. No SSN or other personal unique identifier data shall be stored on individuals’ Government-furnished PCs or laptops. Where SSNs are present on the NDU network, access to such repositories shall be controlled and restricted to only those with a “need to know.” No PII shall be stored in accessible collaboration spaces, such as SharePoint. Should there be a need to transmit PII via email, the email must be encrypted.

(3) The SCOP tracks all PII being collected by the university in a portfolio of “PII Holdings.” ITD conducted an initial evaluation of PII holdings in 2017. This analysis is in the document titled “NDU Data Requirements Specification” (Reference (p)). To keep this portfolio up to date, the SCOP conducts a survey of all components and reviews these PII holdings annually to ensure that only identified PII is collected and retained, and that the PII continues to be necessary to accomplish the legally authorized purpose. All NDU component leadership is responsible for immediately notifying the SCOP if the nature or general content of PII holdings for their component changes throughout the year. They must also work with the SCOP to ensure proper consent is recorded from individuals regarding collection of their PII, in accordance with this document section titled “Consent (IP-1).”

b. Locate / Remove / Redact / Anonymize PII (DM-1 (1)).

(1) System Owners, where feasible and within the limits of technology, locate and remove/redact specified PII and/or use anonymization and de-identification techniques to permit use of the retained information while reducing its sensitivity and reducing the risk resulting from disclosure. This is accomplished through Data Loss Prevention Controls and rule sets that automatically detect PII. For NDU, it is especially important to configure tools in the public cloud (DISA Impact Level 2) to detect instances of disallowed PII. All data stored in any NDU systems that are in violation of DoD and NDU data policy must be removed by the owner. Location and removal is accomplished using the following procedure:

(a) ITD performs a review (either with an automated tool or manual spot check) and an ITD POC provides notification to individuals who are not compliant. Account holders should also

periodically perform a self-check and immediately purge any data not compliant with the guidelines.

(b) If data files are identified by ITD as being non-compliant, the user/owner must remove the data within three (3) days of notification.

(c) 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.

(d) If any NDU user 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 prohibited information.

(2) The only permissible PII data in NDU systems for collection or retention are data which are recorded on the NDU published System of Records Notice (SORN). This data includes: Name, address, date of birth, citizenship, race, Social Security Number (SSN), phone numbers, e-mail addresses, disability information, student identification number, grade/rank, branch of service or civilian agency, years of Federal service, school attended and years of attendance, security clearance granted and date, biographical data, course/section assignment, prior education, and academic data.

(3) All NDU components, staff, faculty and students are responsible for being vigilant and following policies regarding safe handling of PII. It should not be assumed that automated solutions will serve as the only protection or will catch all policy violations.

c. Data Retention and Disposal (DM-2). The NDU RM:

(1) Retains each collection of PII to fulfill the purpose(s) identified in the SORN or as required by law, as follows:

(a) Individual and class academic records are destroyed after 40 years.

(b) Records pertaining to extension courses are held indefinitely before being retired to the National Personnel Records Center, St. Louis, MO.

(c) Individual training records are destroyed annually.

(d) Management reports are destroyed as soon as they are no longer needed.

(2) Disposes of, destroys, erases, and/or anonymizes the PII, regardless of the method of storage, in accordance with a NARA-approved record retention schedule and in a manner that prevents loss, theft, misuse, or unauthorized access

(3) Uses media destruction (MD) methods to ensure secure deletion or destruction of PII (including originals, copies, and archived records) in accordance with DoD 5400.11-R (Reference

(h)). For more information about Media Destruction, refer to the NDU Media Protection Policy and Procedures (MP-1) (Reference (o)).

d. Minimization of PII Used in Testing, Training, and Research (DM-3). It is NDU policy to not use PII for testing, training, and research. Should an exception to this policy be needed, address the request to the SCOP. An evaluation will be made by the SCOP and CISO as to whether a waiver for such activity would be granted. In such cases, the SCOP must ensure the requestor has implemented controls to protect PII used for testing, training, and research.

e. Risk Minimization Techniques (DM-3 (1)). It is NDU policy to not use PII for testing, training, and research. Should an exception to this policy be granted by the SCOP and CISO, a risk management plan is required from the requestor of the testing, training, and/or research activity.

3.6. INDIVIDUAL PARTICIPATION AND REDRESS (IP). IP controls address the need to make individuals active participants in the decision-making process regarding the collection and use of their PII. By providing individuals with access to PII and the ability to have their PII corrected or amended, as appropriate.

a. Consent (IP-1).

(1) It is NDU standard practice to minimize the collection of PII unless it is required to meet the mission of the university and/or properly service the student lifecycle. When a new determination is made that PII must be collected, the component that wishes to collect the information must contact the SCOP for guidance and tracking.

(2) Where feasible and appropriate, NDU provides the means for individuals to provide consent authorizing the collection, use, maintaining, and sharing of PII prior to its collection. Methods of obtaining consent include:

(a) Electronic signature through the academic application process, on applications with appropriate privacy statement markings

(b) Wet signature or hand-written signature on paper applications and forms that contain appropriate privacy statement markings.

(3) New uses or disclosure of previously collected PII are rare and should be coordinated directly with the SCOP. Should this become necessary, NDU shall obtain authorization/consent from individuals prior to any new uses or disclosure of previously collected PII. This can be done via electronic or hand-written consent forms distributed through NDU email for faculty and staff, or NDU academic systems for students. If consent is not feasible, then notice shall be posted on the NDU SharePoint Portal and NDU academic systems. In this way, the SCOP ensures that individuals are aware of, and where feasible, consent to, all uses of PII not initially described in the public notice that was in effect at the time NDU collected the PII.

(4) All forms of PII collection (online, paper forms, etc.) provide appropriate means for individuals to understand the consequences of decisions to approve or decline the authorization of the collection, use, dissemination, and retention of PII through privacy notices, privacy training and

other awareness activities, by using the standard Privacy Statements found in Appendix A and Appendix B.

(5) All NDU systems display a standard Terms of Use notice (example in Appendix C) to notify users that they should have no expectation of complete privacy when using a U.S. Government System. However, this Terms of Use statement does not cover PII and does not give NDU explicit permission to collect PII without the additional consent described in this section.

b. Mechanisms Supporting Itemized or Tiered Consent (IP-1 (1)). The SCOP implements mechanisms to support itemized or tiered consent for specific uses of data.

c. Individual Access (IP-2).

(1) An individual may request access to their PII held by NDU in its system(s) of records through submitting a Freedom of Information Act (FOIA) request to:

<p style="text-align: center;">FOIA Contact OSD/JS FOIA Requester Service Center, Office of Freedom of Information 1155 Defense Pentagon Washington, DC 20301-1155</p> <p style="text-align: center;">(866) 574-4970 (Telephone) (571) 372-0500 (Fax)</p> <p style="text-align: center;">whs.mc-alex.esd.mbx.osd-js-foia-requester-service-center@mail.mil (Request via Email)</p> <p style="text-align: center;">FOIA Requester Service Center: Phone: (866) 574-4970</p> <p style="text-align: center;">Website: http://www.dod.gov/pubs/foi/</p> <p style="text-align: center;">Online Request Form: http://www.dod.gov/pubs/foi/foiareq.html</p>
--

(2) The SCOP, upon receipt of a FOIA request:

(a) Provides individuals the ability to have access to their PII maintained in its system(s) of records

(b) Publishes rules and regulations governing how individuals may request access to records maintained in a Privacy Act system of records

(c) Publishes access procedures in System of Records Notices (SORNs)

(d) Adheres to Privacy Act requirements and OMB policies and guidance for the proper processing of Privacy Act requests

d. Redress (IP-3).

(1) Requests for correction of PII related to a students' academic record are directed to the Registrar for the appropriate NDU component, or NDU Academic Affairs. AA notifies the individual when the correction is complete, where feasible.

(2) For correction of all other types of records in NDU information systems, the SCOP facilitates the correction through the appropriate SO using the following process:

(a) Individuals that wish to have inaccurate PII maintained by NDU corrected or amended, as appropriate, may submit the request in writing.

(b) The SCOP works with the SO to make the appropriate corrections.

(c) The SCOP disseminates corrections or amendments using the following procedures:

1. The SCOP applies safeguards to the information before disseminating. All procedures for safeguarding of PII as defined in this policy document shall be followed for the transfer of PII, including FIPS 140 encryption.
2. The corrections of the PII are disseminated only to other authorized users of the PII, including but not limited to the NDU Registrar and/or the SO of academic systems. In general, there are no external information-sharing partners of NDU data.
3. All dissemination is completed in accordance with DoD 5400.11 (Reference (g)) and DoD 5400.11-R (Reference (h)).

(d) Where feasible, and in accordance DoD 5400.11 (Reference (g)) and DoD 5400.11-R (Reference (h)) the SCOP notifies the affected individual(s) that their information has been corrected or amended. This can be done by:

1. Electronic or written communication to individuals notifying them of the correction
2. Electronic posting (such as to the SharePoint or Academic portals) notifying a large group that mass corrections have been made

e. Complaint Management (IP-4). Complaints, concerns, or questions from individuals about NDU privacy practices may be directed to the SCOP. The SCOP will acknowledge such communication within 5 business days of receipt.

f. Response Times (IP-4 (1)). The SCOP ensures that NDU responds to complaints, concerns, or questions from individuals within seven business days. This response may be via email or other means as the SCOP deems appropriate.

3.7 SECURITY (SE). SE controls ensure that technical, physical, and administrative safeguards are in place to protect PII collected or maintained by organizations against loss, unauthorized access, or disclosure, and to ensure that planning and responses to privacy incidents comply with OMB policies and guidance. The controls in this family are implemented in coordination with information security personnel.

a. Inventory of PII (SE-1).

(1) The portfolio of PII holdings is in the document titled “NDU Data Requirements Specification” (Reference (p)). This inventory includes:

(a) Programs that collect, use, maintain or share PII

(b) Information systems that collect, use, maintain or share PII

(2) The SCOP maintains and updates the inventory every three years, commensurate with the RMF Continuous Monitoring and ATO accreditation cycle, or more often if there is a system or data change impacting the inventory. This inventory is updated by validating contents with the NDU components, collecting their updates and additions, and incorporating them into the master inventory.

(3) When the portfolio is updated, the SCOP provides updates of the PII inventory to the CIO or information security official within 90 days to support the establishment of information security requirements for all new or modified Information Systems containing PII. Similarly, if ITD approves a new system for deployment through its normal Configuration Management process, the CISO shall inform the SCOP for update of the PII Holdings inventory if it is impacted.

b. Privacy Incident Response (SE-2).

(1) The SCOP is responsible for implementing and maintaining the NDU Privacy Incident Response Plan described in this section. The steps in the plan augment the DoD procedures outlined in DoD 5400-11-R. The SCOP should coordinate with the CISO and/or ISSM for all incidents, and also invoke the NDU Incident Response Policy and Procedures (IR-1) (Reference (q)) as appropriate.

(2) Incidents regarding spillage are immediately reported to the SCOP. The SCOP provides an organized and effective response to privacy incidents in accordance with the following schedule:

PII Spillage Incident Response Timeline	
Within one hour	Incident discovery and call to NDU COS/S/CIO, Notify USCERT Team
Within several hours	Notify individuals on the Notification (Internal to NDU) list below
Within 24 hours	Notify Component Official for Privacy
Within 48 hours	Notify WHS Records Privacy and Classification Division of Defense Privacy Office, then they report to DCLPTD
Within +/- 10 Days	Notify individuals affected as soon as possible, NLT 10 Working days. The 10-day period begins after the loss is discovered and ID ascertained (the Component is able to determine the identities of the individuals whose records were lost)

(3) Reporting Requirements: when a loss, theft, or compromise of information occurs, the breach shall immediately be reported to the NDU Security Office (202-685-2605), NDU Chief Information Office (202-685-4736), and NDU Chief of Staff (202-685-3927). The date of the loss, circumstances of the loss, person(s) involved will be provided. Do not provide specific information via e-mail or un-secure phone until told to do so. If and when e-mail traffic concerning the breach is sent, include NDU IT at NDU-IA@ndu.edu.

(4) Notification (INTERNAL TO NDU): The SCOP will notify the following parties when an incident occurs:

NDU Chief of Staff (202-685-3927)

Legal (202-2685-2015)
CIO (202-685-4736)
Security (202-685-3835)
Army Research Lab (410-278-8940)

(5) Notification to Individuals: if records containing personal information are lost, stolen, or compromised the potential exists that the records may be used for unlawful purposes, such as identity theft, fraud, stalking, etc. The personal impact on the affected individual may be severe if the records are misused. To assist the individual, the Component shall promptly notify the individual of any loss, theft, or compromise.

(a) The notification shall be made whenever a breach occurs that involves personal information pertaining to a service member, civilian employee (appropriated or non-appropriated fund), military retiree, family member, DoD contractor, other persons that are affiliated with the Component (e.g., volunteers), and/or any other member of the public on whom information is maintained by the Component or by a contractor on behalf of the Component.

(b) The notification shall be made as soon as possible, but not later than 10 working days after the loss, theft, or compromise is discovered and the identities of the individuals ascertained. The 10-day period begins after the Component is able to determine the identities of the individuals whose records were lost.

(c) If the Component is only able to identify some but not all of the affected individuals, notification shall be given to those that can be identified with follow-up notifications made to those subsequently identified.

(d) If the Component cannot readily identify the affected individuals or will not be able to identify the individuals, the Component shall provide a generalized notice to the potentially impacted population by whatever means the Component believes is most likely to reach the affected individuals.

(e) When personal information is maintained by a DoD contractor on behalf of the Component, the contractor shall notify the Component immediately upon discovery that a loss, theft, or compromise has occurred.

(f) The Component shall determine whether the Component or the contractor shall make the required notification.

(g) The notice to the individual, at a minimum, shall include the following:

1. The specific data that was involved. It is insufficient to simply state that personal information has been lost. Where names, Social Security Numbers (SSNs), and dates of birth are involved, it is critical that the individual be advised that these data elements potentially have been compromised.

2. The facts and circumstances surrounding the loss, theft, or compromise. The description of the loss should be sufficiently detailed so that the individual clearly understands how the compromise occurred.

3. What protective actions the Component is taking or the individual can take to mitigate against potential future harm, including referring the individual to the Federal Trade Commission's public web site on identity theft at http://www.consumer.gov/idtheft/con_steps.htm.

3.8. TRANSPARENCY (TR). TR controls ensure that NDU provides public notice of their information practices and the privacy impact of their programs and activities.

a. Privacy Notice (TR-1).

(1) If a system collects PII, the System Owner provides effective notice to the public and to individuals. This is accomplished by publishing the SORNs (see control TR-2). The SORN includes information regarding:

(a) Its activities that impact privacy, including its collection, use, sharing, safeguarding, maintenance, and disposal of PII

(b) Authority for collecting PII

(c) The choices individuals may have regarding how NDU uses PII and the consequences of exercising or not exercising those choices

(d) The ability to access and have PII amended or corrected if necessary

(2) A sample NDU System Privacy Notice is found in Appendix A. The privacy notice provides effective notice to individuals before collection of PII on an information system or form and describes:

(a) The PII that NDU collects and the purpose(s) for which it collects that information

(b) How NDU uses PII internally

(c) Whether NDU shares PII with external entities, the categories of those entities, and the purposes for such sharing. In general, there are no external information-sharing partners of NDU data.

(d) Whether individuals have the ability to consent to specific uses or sharing of PII and how to exercise any such consent

(e) How individuals may obtain access to PII

(f) How the PII will be protected

(3) The SCOP revises NDU's public notices to reflect changes in practice or policy that affect PII or changes in its activities that impact privacy, before or as soon as practicable after the change.

b. Real-Time or Layered Notice (TR-1 (1)). For systems that collect PII, the System Owner provides real-time and/or layered notice. This can take the form of a "splash screen," pop-up notice or other immediate notice to the end user.

c. System of Records Notices and Privacy Act Statements (TR-2).

(1) All System of Records Notices (SORNs) must be kept current using the following process:

(a) The SCOP reviews SORNs at least every two years and updates as necessary. This review process includes checking the PII inventory to ensure no new PII is collected that needs to be recorded and published for public record in the SORN. The SCOP also performs a general check to ensure all SORN information, including published contact information, is still current.

(b) When updates are identified, the SCOP develops, updates and sends applicable SORNs to the WHS Records Privacy and Declassification Division for review.

(c) WHS Records Privacy and Declassification Division reviews and sends the SORN(s) to Defense Privacy Civil Liberties and Transparency Division (DPCLTD) who publishes in the Federal Register, subject to required oversight processes (including review and approval by the Senior Agency Official for Privacy (SAOP)), for systems containing PII.

(d) SORNs are only required for those systems that are NDU-specific. Otherwise, it may be assumed that NDU inherits all SORNs from the Office of the Secretary of Defense and the Chairman of the Joint Chiefs of Staff.

(2) The SCOP ensures that NDU includes Privacy Act Statements on NDU forms that collect PII, or on separate forms that can be retained by individuals, to provide additional formal notice to individuals from whom the information is being collected.

d. Public Website Publication (TR-2 (1)).

(1) The SCOP works with DPCLTD personnel to publish SORNs on the DPCLTD public website. This website contains a searchable archive of all SORNs for DoD components.

(2) Upon approval from the DPCLTD, the SCOP also sends the SORN to the NDU Knowledge Management Officer for publication on the NDU Public Web Site. (TR 2.2)

e. Dissemination of Privacy Program Information (TR-3).

(1) The SCOP ensures that the public has access to information about NDU privacy activities through SORNs published in accordance with control TR-2(1).

(2) The SCOP also publishes Section 1 of the Privacy Impact Assessment (PIA) (DD Form 2930) to the NDU public website in accordance with DoDD 5400.11 (Reference (g)), DoD 5400.11-R (Reference (h)), and DoDI 5400.16 (Reference (i)). The web site also contains the name, phone number and email address of the SCOP so the public is able to communicate with them.

(3) NDU privacy practices are also publicly available because this policy document is releasable to the public and is also published on the NDU public web site.

3.9 USE LIMITATION (UL). UL controls ensure that NDU only uses PII either as specified in their public notices, in a manner compatible with those specified purposes, or as otherwise permitted by law. Implementation of the UL controls ensures that the scope of PII use is limited accordingly.

a. Internal Use (UL-1). The SCOP ensures that NDU uses PII internally only for the authorized purpose(s) identified in the Privacy Act and/or in NDU public notices, as described within this Policy and Procedures document. Should any other use occur, the SCOP shall handle the incident in accordance with the Incident Response section of this policy.

b. Information Sharing With Third Parties (UL-2).

(1) The SCOP ensures that NDU shares PII externally, only for the authorized purposes identified in the Privacy Act and/or described in its notice(s) or for a purpose that is compatible with those purposes. In general, NDU does not share PII with external partners.

(2) Where appropriate and if needed in the future to share PII information:

(a) NDU will enter into Memoranda of Understanding, Memoranda of Agreement, Letters of Intent, Computer Matching Agreements, or similar agreements, with third parties that specifically describe the PII covered and specifically enumerate the purposes for which the PII may be used.

(b) The SCOP will monitor, audit, and train its staff on the authorized sharing of PII with third parties and on the consequences of unauthorized use or sharing of PII.

(c) The SCOP will evaluate any proposed new instances of sharing PII with third parties to assess whether the sharing is authorized and whether additional or new public notice is required. The SCOP will recommend to the COO whether such agreements are compliant with DoD cybersecurity policies and whether NDU should proceed with the given agreement.

GLOSSARY

A common Cybersecurity language lexicon is defined in Reference (d).

G.1. ACRONYMS.

AO	Authorizing Official
ATO	Authority to Operate
BLCR	Baseline Cybersecurity Requirements
CIO	Chief Information Officer
CISO	Chief Information Security Officer
COO	Chief Operating Officer
CPO	Component Privacy Officer
DA&M	Director of Administration and Management
DPCLTD	Defense Privacy Civil Liberties and Transparency Division
IAW	In Accordance With
IS	Information System
ISSO	Information System Security Officer
ITD	Information Technology Directorate
NARA	National Archives and Records Administration
NDU	National Defense University
PIA	Privacy Impact Assessment
PII	Personally Identifiable Information
PMO	Project Management Office
SCOP	Senior Component Official for Privacy
SIA	Security Impact Analysis
SSN	Social Security Number
SO	System Owner
SORN	System of Records Notice
USG	U.S. Government

G.2. DEFINITIONS.

Personally Identifiable Information. DoD 5400.11, DoD Privacy Program, defines PII as: Information used to distinguish or trace an individual's identity, such as name, social security number, date and place of birth, mother's maiden name, biometric records, home phone numbers, other demographic, personnel, medical, and financial information. PII includes any information that

is linked or linkable to a specified individual, alone, or when combined with other personal or identifying information.

REFERENCES

- (a) 5 U.S. Code § 552a, Privacy Act of 1974
- (b) 10 U.S.C. 2165, National Defense University
- (c) 10 U.S.C. 2163 Degree Granting Authority for National Defense University
- (d) Committee on National Security Systems Instruction (CNSSI) 4009, “National Information Assurance Glossary,” April 6, 2015
- (e) DD Form 2930, “Privacy Impact Assessment,” November 2008
- (f) DoDI 5015.02, “DoD Records Management Program,” February 24, 2015
- (g) DoD 5400.11, “DoD Privacy Program,” October 29, 2014
- (h) DoD 5400.11-R, “Department of Defense Privacy Program,” May 14, 2007
- (i) DoDI 5400.16, “DoD Privacy Impact Assessment (PIA) Guidance,” August 11, 2017
- (j) Executive Order 9397, “Numbering System For Federal Accounts Relating To Individual Persons,” November 22, 1943, as amended in Executive Order 13478, November 18, 2008
- (k) National Defense University (NDU), Information Technology Directorate (ITD), “Baseline Cybersecurity Requirements (BLCR) for Information Technology,” March 2017
- (l) National Defense University (NDU), Information Technology Directorate (ITD), “Contact with Security Groups and Associations (PM-15),” April 2017
- (m) National Defense University (NDU), Information Technology Directorate (ITD), “Enterprise Information Architecture (PM-7),” March 2017
- (n) National Defense University (NDU), Information Technology Directorate (ITD), “ITD Requirements Vetting and PMO Process,” May 2017
- (o) National Defense University (NDU), Information Technology Directorate (ITD), “Media Protection Policy and Procedures (MP-1),” May 2018
- (p) National Defense University (NDU), Information Technology Directorate (ITD), “NDU Data Requirements Specification,” February 2017
- (q) National Defense University (NDU), Information Technology Directorate (ITD), “NDU Incident Response Policy and Procedures (IR-1),” May 2018

- (r) National Defense University (NDU), Information Technology Directorate (ITD), “NDU Risk Management Strategy (PM-9),” May 2018
- (s) National Defense University, Office of the Chief Information Officer, “NDU Instruction 5015.16: Records Management,” December 12, 2017
- (t) NIST Special Publication 800-122, “Guide to Protecting the Confidentiality of Personally Identifiable Information (PII),” April 6, 2010
- (u) Office of Management and Budget (OMB) Memorandum M-16-24, “Role and Designation of Senior Agency Officials for Privacy,” September 15, 20

APPENDIX A: SAMPLE PRIVACY STATEMENT FOR SYSTEMS.

All systems shall display a privacy statement and disclaimer to users before logging in. Below is a sample that is compliant with all DoD and U.S. Government guidelines.

PRIVACY ACT STATEMENT

AUTHORITY: 10 U.S.C. 2165, National Defense University; 10 U.S.C. 2163 Degree Granting Authority for National Defense University and E.O. 9397, as amended (SSN).

PURPOSE: The data provided will be used to update your National Defense University (NDU) record. NDU data are used to authenticate and identify NDU personnel and students; track academic enrollment, assignments, progress, and assessments; track personnel records and actions; create academic transcripts and related reports; facilitate award of degrees and credentials; conduct analysis for regional and DoD academic accreditations; and create reports for University leadership to aid in the development of effective curricula.

ROUTINE USES: Data are shared with other Federal/State agencies and contractors for the purpose of communicating educational credentials and accrediting University programs.

DISCLOSURE: Voluntary. However, if data in NDU systems are not up to date, your NDU entitlements/privileges and the ability of NDU systems to identify you as an NDU-affiliated person could be delayed or inaccurate. The production of accurate academic transcripts may not be possible. Home addresses will be used for mustering in the event of an officially declared manmade or natural disaster (DoDI 3001.02) and for notification of a Privacy compromise, loss or stolen (breached) personally identifiable information (PII). If addresses are not correct these two requirements will not be performed with accuracy as to your location.

APPENDIX B: SAMPLE PRIVACY STATEMENT FOR FORMS.

PRIVACY ACT STATEMENT

AUTHORITY: 10 U.S.C. 2165, National Defense University; 10 U.S.C. 2163 Degree Granting Authority for National Defense University and E.O. 9397, as amended (SSN).

PURPOSE: The data provided will be used to update your National Defense University (NDU) record for _____.

ROUTINE USES: Data are shared with _____ for the purpose of _____.

DISCLOSURE: Voluntary. However, if data is not provided, _____.

APPENDIX C: SAMPLE TERMS OF USE FOR NDU APPLICATIONS.

The wording below is a sample “Terms of Use” statement to be displayed on all NDU Applications.

YOU ARE ACCESSING A U.S. GOVERNMENT (USG) INFORMATION SYSTEM (IS)
THAT IS PROVIDED FOR USG-AUTHORIZED USE ONLY.

By using this IS (which includes any device attached to this IS), you consent to the following conditions:

- The USG routinely intercepts and monitors communications on this IS for purposes including, but not limited to, penetration testing, COMSEC monitoring, network operations and defense, personnel misconduct (PM), law enforcement (LE), and counterintelligence (CI) investigations.
- At any time, the USG may inspect and seize data stored on this IS.
- Communications using, or data stored on, this IS are not private, are subject to routine monitoring, interception, and search, and may be disclosed or used for any USG-authorized purpose.
- This IS includes security measures (e.g., authentication and access controls) to protect USG interests—not for your personal benefit or privacy.
- Notwithstanding the above, using this IS does not constitute consent to PM, LE or CI investigative searching or monitoring of the content of privileged communications, or work product, related to personal representation or services by attorneys, psychotherapists, or clergy, and their assistants. Such communications and work product are private and confidential. See User Agreement for details.

APPENDIX D: DOCUMENT CONTROL TABLE.

DOCUMENT CONTROL			
Version #	Implemented By	Revision Date	Description
1.0	Gina Nairn	04/18/2017	Initial Revision
1.1	Gina Nairn	6/8/2017	Revisions throughout document after collecting input from NDU Director of Security
1.2	Gina Nairn	6/26/2017	Final revision after CISO review, ready for CIO review/signature
--	--		Signed by CIO 6/29/2017
2.0	Tanja Katrin	1/29/2018	Reformatted with NDU Issuance template and prepared for COO review and signature
2.1	Gina Nairn	1/30/2018	Added control information for RMF compliance list.
2.2	Gina Nairn	4/24/2018	Changed references to “Chief Privacy Officer” to “Component Privacy Officer”
2.3	Gina Nairn	5/21/2018	Annual review. Added content throughout to ensure compliance with RMF controls.
2.4	Gina Nairn	5/25/2018	Updates to reporting requirements and PII Spillage timeline requirements, per inputs from WHS Records Privacy and Declassification Division review
2.5	Gina Nairn	5/29/2018	Minor update to DI section to clarify when quality checks are performed during the student lifecycle.
2.6	Gina Nairn	6/12/2018	Replaced all references to “CSOP” with “SCOP” to be consistent with OSD guidance. Revised process to publish SORN based on inputs received from WHS Records Privacy and Declassification Division.
2.7	Gina Nairn	6/20/2018	Modified SE-1 to reflect that PII Inventory is updated every 3 years, consistent with DoD policy. (Previously this said “annual.”)
2.8	Gina Nairn	6/26/2018	Minor update to AR-4 to show privacy control audits are conducted in the ATO review cycle, every three years. Audit records are maintained in eMASS.
2.9	Tanja Katrin	7/6/2018	Minor format revisions.
2.10	--	7/6/2018	Version reviewed and signed by COO.