Attachment 5 – Military Personnel Data System (MilPDS) User Agreement

As a user of MilPDS, I acknowledge my responsibility and I understand the system security-related rules, procedures, or practices outlined below and the conditions related to the appropriate use of Government Information Systems (IS). I certify that I have completed the applicable annual cybersecurity awareness training and my training is current. Air Force Instruction (AFI) 17-130, Cybersecurity Program Management applies, and I have reviewed the "MilPDS Access Control" policy in PSDM 23-39. I further understand that I can be held criminally liable for disclosing sensitive data in violation of the Privacy Act of 1974. As a user of MilPDS, I agree to:

1. **I WILL adhere to and actively support all legal, regulatory, command, and training requirements**:

- Effective 1 June 2023, if as a **NEW** user to MilPDS, I will successfully complete the MilPDS ***AFQTPXXXXX-251B, MilPDS User 101 Fundamentals course:*** ***https://lms-jets.cce.af.mil/moodle/user/view.php?id=72437&course=12006*** before requesting access to MilPDS and in addition to completing the M*ilPDS User 101 Fundamentals Course*, at a minimum all **NEW** users filling a funded authorization under FACs: 10A1, 10W100, 10G100, 10HI, 10S100, 5540, and 51S00 on the unit UMD/UPMR must also successfully complete the ***Commander's Support Staff (CSS) Course***, ***AFJQS3FXXX-252A***: ***https://lms-jets.cce.af.mil/moodle/course/view.php?id=12925*** except for UDMs/UTMs assigned to these FACs before receiving access to MilPDS. MPF Commanders and Chiefs may enforce more stringent and robust training requirements to achieve desired goals
- I waive my expectation of privacy in my Air Force electronic communications. This is not a waiver of my rights to attorney-client privilege, medical information privacy, or the privacy afforded communications with religious officials/chaplains
- I will observe all software license agreements and federal copyright laws
- I will encrypt sign any message containing For Official use Only (FOUO) or Personally Identifiable Information (PII)
- I will promptly report all security incidents to my appointed MilPDS-DSA/PSM in accordance with Air Force policy, PSDM 22-32
- I **MUST FIRST** register with the Air Force Identity Services—AFID Identity Management Portal: **https://imp.afds.af.mil/default.aspx** **or** for Non-AF assets visit **https://epi.afds.af.mil/nonaf/** prior to requesting a MilPDS account. This applies to **ALL** users of the MilPDS; regardless, of service, component, or category affiliation
- I understand that I **MUST** select my "**Authentication Certificate**" whenever prompted to successfully gain access to the MilPDS
- As a MilPDS user, I understand that I may have to personally contact the Defense Manpower Data Center (DMDC) if my CAC certificates are either missing or corrupted before I can successfully gain access to the MilPDS
- As a MilPDS user, I understand I **MUST** follow and comply with **ALL** AFIs, PSDMs, and PSDGs when accessing and/or updating, changing, or deleting information/data in the MilPDS and all that applicable source document(s) used for supporting the update(s) were reviewed for accuracy, completeness, and the proper authority prior to making the update in MilPDS
- I **WILL** digitally or electronically complete the DD2875 (SAAR) along with this User Agreement (UA) IAW procedural guidance and obtain all necessary digital/electronic signatures prior to sending to my MilPDS-DSA/PSM to create a new account or assign role(s) for a pre-existing MilPDS account
- As a MilPDS user, I understand I **WILL NOT** make any updates to my own personnel record in MilPDS that could or may cause an unfair advantage over other Airmen for those HR-related programs such as promotions, assignments, retention, and those that directly affect pay, benefits, and entitlements. I further understand that I can make updates using MilPDS to my own personnel record for information or data normally reserved to self-service applications contained in the vMPF or similar self-service applications

Attachment 5 – Military Personnel Data System (MilPDS) User Agreement

- **I WILL** protect all PII related data/information derived from MilPDS IAW DoDI 5400.11, "DoD Privacy and Civil Liberties Programs"

2. **I WILL use the system in a manner that protects information confidentiality, integrity and/or availability**.

- I will not store or process classified information on any system not approved for classified processing
- I will protect my Common Access Card (CAC) token from loss, compromise, or premature destruction. I will not share my token/credentials with anyone, use another person's token/credentials, or use a computer or terminal on behalf of another person
- I will protect my Personal Identification Numbers and credentials from disclosure. I will not post or write these down in my workspace
- I will lock or log-off my computer or terminal any time I walk away
- I will not disclose any non-public Air Force or DoD information to unauthorized individuals
- I understand that everything done using my Common Access Card (CAC) or Personal Identification Number (PIN) will be regarded as having been done by me
- I will immediately notify my appointed MilPDS-DSA of all periods of transition such as permanent change of assignment/station (PCA/PCS), separation, retirement, deployment, loss of employment, or component category affiliation change prior to my departure
- I understand the MilPDS system rules of behavior such as idle accounts or inactive accounts for 35-days will change my account status from "Active to Inactive" and require me to contact my appointed M-DSA/PSM to unlock my account

3. **I WILL NOT attempt to exceed my authorized privileges**.

- I will not access, research, or change any account, file, record, or application not required to perform my job than my current level of authorized access in accordance with (IAW) PSDM 23-39 or the current MilPDS Access Control policy currently in place than allows me
- I will not modify the operating system configuration on Air Force Information Technology without proper approval
- I will not move equipment, add or exchange system components without authorization by the appropriate level of approval of my local systems manager or local hardware custodial personnel

I promise to comply with all rules, procedures, or practices to the best of my ability and understand that the following statements reflect mandatory behavioral norms and standards of acceptable use of Air Force Information Technology (IT).

10/17/2023

Digital Signature of MilPDS User	Date

BUNNY, BUGS E.	TSGT/PSM MANAGER

Printed Name (Last, First, MI)	Rank/Position

341 FSS/FSPJ / MALMSTROM AFB, MT 59405

Unit and Location of MilPDS User