Cybersecurity and Privacy Rules of Behavior (ROB)

I. Introduction

These Rules of Behavior (ROB) for Users pertain to the use, security, and acceptable level of risk for HIDTA PIP system. Each user is responsible for helping to ensure the security and privacy of HIDTA PIP information system and data.

The intent of this ROB is to acknowledge receipt and understanding by HIDTA PIP users of applicable cybersecurity requirements and responsibilities. These requirements include, but are not limited to, the Office of Management and Budget (OMB) Circular A-130, the Privacy Act of 1974, applicable Department and/or AHIDTA policies.

Who is covered by these rules?

These rules apply to all personnel who have logical access to HIDTA PIP system and information, referred to as Users. All users are required to review and provide signature or electronic verification acknowledging compliance with these rules.

Users will be held responsible for compromising HIDTA PIP information through negligence or willful acts. Users must use caution and follow all statutory and regulatory access, use, maintenance, and disclosure restrictions, as well as adhere to AHIDTA policies regarding the exchange of access-restricted information including personally identifiable and controlled unclassified information. Failure to comply with the rules and responsibilities listed in this ROB may result in appropriate sanctions, including but not limited to: remedial training; loss of access to information; loss of a security clearance; verbal or written warning; termination of employment; and civil or criminal prosecution.

II. User Responsibilities

A. General

1. Comply with all Federal laws, and AHIDTA policies and requirements, including Department Orders, Policy Statements, and Standards. Use HIDTA PIP system and information for lawful, official use, and authorized purposes only.

2. Ensure individuals have the proper clearance, authorization, and need-to-know before providing access to HIDTA PIP information and information system.

3. Read and accept the security warning banner that appears prior to logging onto the system. Acknowledgment of this ROB also indicates consent to monitoring, recording, and collection of data for law enforcement purposes.

4. Screen-lock or log off when leaving the work area.

5. Always keep your identification and authentication (I&A) credentials secure.

6. Ensure that all sensitive information in hardcopy or electronic form is removed from the workspace and secured in a drawer when the desk is unoccupied at the end of the workday.

7. Adhere to Separation of Duties principles. Avoid conflict of interest in responsibilities, roles, and functions within a system or application.

8. Do not use anonymizer sites on the internet or bypass the security mechanisms designed to protect system from malicious internet sites unless authorized for official purposes.

9. Do not post AHIDTA official business information on public websites or social media unless in accordance with applicable policies and explicitly authorized for your official duties (e.g., Public Affairs Office).

10. Do not post information on social media or public websites, which allows unauthorized users to infer or obtain non-public information (e.g., system account information, sensitive personally identifiable information (PII), project status, etc.).

11. Protect and safeguard all HIDTA information commensurate with the sensitivity and value of the data at risk, including encrypting all sensitive PII (as defined below) before sending to third parties outside of AHIDTA.

12. Protect and safeguard all HIDTA information and information system from unauthorized access including unauthorized or inadvertent modification, disclosure, damage, destruction, loss, theft, denial of service, and improper sanitization or use.

13. Ensure that all HIDTA data on authorized removable media (e.g., thumb drives, removable hard drives, and CD/DVD), laptops, tablets, and mobile devices (e.g., smartphones and netbooks) are encrypted with an approved solution.

14. Handle all HIDTA data as Sensitive unless designated as non-sensitive.

15. Report any anomalous or unusual behavior and discovered or suspected security incidents to an appropriate point of contact (POC) (e.g., Help Desk, Incident Response Representative, Security Manager, Supervisor).

16. Ensure that you complete all required training in accordance with current policies.

17. Follow all Department level policies related to user responsibilities for the recording of information into the Department’s recordkeeping systems and comply with applicable records retention schedules.

B. Passwords

18. Comply with password policies (e.g, must be at least 12 characters, contains upper-case, lower-case, numeric, and special characters (e.g. ~ ! @ #$ % ^ & * ( ) _ + = - ‘ [] / ? > <)).

19. Change default passwords upon receipt from a system administrator.

20. Do not share account passwords with anyone.

21. Avoid using the same password for multiple accounts.

C. Hardware

22 Do not add, modify, remove hardware, or connect unauthorized accessories or communications connections to HIDTA resources unless specifically authorized.

D. Software

23. Do not copy or distribute protected intellectual property without permission or license from the copyright owner (e.g., music, software, documentation, and other copyrighted materials). Use only licensed and authorized software.

24. Do not install or update any software unless specifically authorized. Submit requests for system changes through the appropriate help desk or configuration management process.

25. Do not attempt to access any electronic audit trails that may exist on the computer unless specifically authorized.

26. Do not change any configurations or settings of the operating system and security-related software or circumvent and test the security controls of the system unless authorized through the documented configuration management procedures.

E. Email Use

27. Limit distribution of email containing HIDTA information only to those who are authorized and need to know the information to perform their job duties.

28. Do not open emails from suspicious sources (e.g., people you do not recognize, know, or normally communicate with) and do not visit untrusted or inappropriate websites, unless authorized for official purposes. Download permissible files only from known and reliable sources and use virus- checking procedures prior to file use.

29. Do not use personal email accounts for AHIDTA business.

F. Mobile Computing and Remote Access

30. Use AHIDTA mobile devices (e.g., laptop, tablet, smartphone) for official business and authorized use only.

31. Always keep AHIDTA mobile devices, portable electronic devices, and removable media secure. When not in use, keep mobile devices, portable electronic devices, and removable media in your physical presence and out of sight.

32. Do not bypass native mobile device operating system controls to gain increased privileges (e.g., jailbreaking or rooting the device).

33. Download and/or install only authorized applications and software on AHIDTA mobile devices, and only from authorized sources.

34. Update all mobile devices, including applications and operating systems to the latest versions and in a timely manner.

35. Immediately report lost or stolen devices (e.g., laptop, phone, tablet, thumb drive) to your appropriate POC (e.g., Help Desk, Incident Response Representative, Security Manager, Supervisor).

36. Follow your organization's telework guidelines when working remotely and/or remotely accessing HIDTA information remotely.

37. Ensure the confidentiality of HIDTA information when using remote access from a non-AHIDTA (public or private).

G. Personally Identifiable Information (PII)

38. PII training requirements:

- Complete mandatory privacy training as part of the on-boarding process and annually thereafter, as required by and within the timeframe set by applicable Department policy.
- Complete role-based privacy training as required by applicable policy, including when the staff member performs specialized privacy roles and responsibilities.
- Complete Cybersecurity Awareness Training or similar security training at least annually.
- Adhere to all PII training and procedures that are specific to your position.

39. No expectation of privacy:

- Understand and consent to having no expectation of privacy regarding any communications transiting, stored on, or traveling to or from HIDTA PIP information system.
- Understand and consent that the communications occurring on HIDTA PIP information system is monitored for any lawful purpose including, but not limited to, monitoring network operations, quality control, employee and user misconduct investigations, and law enforcement investigations.
- Understand and consent that, at any time, the HIDTA PIP may for any lawful purpose monitor, intercept, search, and seize communications or information transiting, stored on, or traveling to or from HIDTA PIP information system.
- Understand and consent that any communications or information transiting, stored on, or traveling to or from HIDTA PIP information system may be disclosed or used for any lawful purpose.

40. Collection of PII:

- Know that "PII" means information that can be used to distinguish or trace an individual's identity, either alone or when combined with other information that is linked or linkable to a specific individual. PII can be in any medium or form, including paper, oral, and electronic.
- Limit the collection of PII to that which is legally authorized, relevant, and reasonably deemed necessary for the proper performance of your responsibilities.
- Collect no information describing how any individual exercises rights guaranteed by the First Amendment unless expressly authorized by statute or by the individual about whom the information is maintained or unless pertinent to and within the scope of an authorized law enforcement activity.

- Follow applicable Department and AHIDTA policies related to responsibilities for the recording or inputting of information into the official recordkeeping systems.

41. Access and use of PII:

- Limit the access and use of PII to that which is legally authorized, relevant, and reasonably deemed necessary for the proper performance of your responsibilities.

42. Maintenance of PII:

- Protect and safeguard PII from loss, compromise, or unauthorized access commensurate with the sensitivity and value of the information and applicable policy.
- Comply with applicable records retention schedules including requirements to destroy, delete, or purge information, and requirements to preserve or produce it.
- Use only authorized and appropriate techniques to erase, delete, or purge PII, or dispose of media containing PII.
- Do not use personally owned information technology such as computers or removable media to store HIDTA PIP related work PII.

43. Disclosure of PII

- When considering whether to disclose PII (including PII within emails) to HIDTA PIP recipient, ensure the recipient has a need-to-know that information to perform his or her job duties, and that such sharing complies with privacy policy and the law.
- When considering whether to disclose PII (including PII within emails) to a non-HIDTA recipient, follow applicable Department and AHIDTA policy and the law, which may also involve keeping an accounting of the date, nature, and purpose of the disclosures, and the name and address of the person or agency to whom the PII is disclosed.
- Do not disclose PII to members of the public (including individuals, or social or news media) unless explicitly allowed by the scope of your duties, applicable Department and AHIDTA policy, and the law.
- Do not post information, including PII, on any social media or public website that allows unauthorized user(s) to infer or obtain non-public information.

44. Breach:

- Know a “breach” is the loss of control, compromise, unauthorized disclosure, unauthorized acquisition, or any similar occurrence where: (1) a person other than an authorized user accesses or potentially accesses PII or (2) an authorized user accesses or potentially accesses PII for an other than authorized purpose.
- Report all suspected or confirmed breaches of PII to your supervisor and AHIDTA Manager as applicable, as soon as possible without unreasonable delay, but no later than 1 hour after discovery.

45. Privacy Act Records:

- Understand that any item, collection, or grouping of information about an individual that is maintained by an agency, and that contains his name, or the identifying number, symbol, or other identifying particular assigned to the individual is a "record" under the Privacy Act of 1974, 5 USC § 552a, which is a subset of PII.

- Understand that most provisions of the Privacy Act apply to Privacy Act records in a "system of records," which the Act defines as "a group of any records under the control of any agency from which information is [routinely] retrieved by the name of the individual or by some identifying number, symbol, or other identifying particular assigned to the individual."
- As required under the Privacy Act, do not maintain records describing how any individual exercises rights guaranteed by the First Amendment unless the collection is expressly authorized by statute or by the individual or the collection is pertinent to and within the scope of an authorized law enforcement activity.
- Understand that the Privacy Act imposes specific requirements regarding notice, collection, use, disclosure, and handling of Privacy Act records. When considering whether to disclose Privacy Act records to recipient, follow applicable Department and/or AHIDTA policy and the law to avoid wrongful disclosure. Remember that need-to-know may not be sufficient justification, by itself, for disclosure of Privacy Act records to a non-AHIDTA recipient. Also, when disclosure is authorized, and when applicable, prepare an accounting of the date, nature, and purpose of the disclosure, and the name and address of the person or agency to whom the Privacy Act record is disclosed.

III. Statement of Acknowledgement

I acknowledge receipt and understand my responsibilities as identified above. Additionally, I acknowledge my responsibility to access, collect, use, maintain, and protect PII in accordance with these rules of behavior and applicable laws, regulations, and policies. I will comply with the Cybersecurity and Privacy ROB. I acknowledge that failure to comply with the ROB may result in appropriate sanctions, including but not limited to: remedial training; verbal or written warning; loss of access to information system; loss of a security clearance; termination of employment; or civil or criminal prosecution.

____ ____________________

Signature Date

Note: Statements of acknowledgement may be made by signature if the ROB is reviewed in hard copy or by electronic acknowledgement if reviewed online. All users are required to review and provide their signature or electronic verification acknowledging compliance with these rules.