IT Security Policy

Effective Date: 01 June 2023

1. Introduction
The IT Security Policy establishes guidelines and procedures to ensure the confidentiality, integrity, and availability of information technology (IT) systems, networks, and data within the Historic Army Aircraft Flight (HAAF). This policy aims to protect HAAF's digital assets, prevent unauthorized access or use, and mitigate the risks associated with potential security breaches.

2. Scope
This policy applies to all employees, volunteers, contractors, and individuals who have access to the HAAF's IT resources, including computer systems, networks, software, data, and digital services.

3. Information Security Responsibilities
a. HAAF Leadership:
- The HAAF leadership is responsible for establishing and enforcing IT security policies, providing appropriate resources and training, and promoting a culture of security awareness among employees, volunteers, and contractors.

b. Employees, Volunteers, and Contractors:
- All individuals accessing the HAAF's IT resources are responsible for adhering to this policy, following security best practices, and promptly reporting any suspected or actual security incidents to the appropriate authority.

4. Data Protection and Privacy
a. Data Classification:
- The HAAF shall classify data based on its sensitivity, criticality, and legal requirements, applying appropriate safeguards accordingly.
- Employees, volunteers, and contractors shall handle and protect data according to its classification level, ensuring confidentiality, integrity, and availability.

b. Personal Data Protection:
- The HAAF shall comply with applicable data protection laws and regulations when collecting, processing, storing, and transmitting personal data.
- Personal data shall be handled securely, accessed only on a need-to-know basis, and protected against unauthorized disclosure or use.

c. Data Backup and Recovery:
- The HAAF shall regularly backup critical data and maintain appropriate backup procedures to facilitate data recovery in the event of data loss or system failure.

5. Access Control
a. User Access:
- User access to the HAAF's IT resources shall be granted based on the principle of least privilege, providing individuals with the minimum level of access necessary to perform their duties.
- User accounts shall be regularly reviewed, and access rights shall be revoked or modified promptly when individuals change roles or leave the HAAF.

b. Password Management:
- Users shall create strong passwords that are unique and confidential, and they shall not share their passwords with others.
- Passwords shall be changed periodically, and multi-factor authentication mechanisms shall be implemented where feasible.

c. System and Network Security:
- The HAAF shall implement appropriate security measures, including firewalls, intrusion detection systems, and antivirus software, to protect its systems and networks from unauthorized access and malware.

6. Physical Security
a. Equipment Protection:
-The HAAF's IT equipment, including computers, servers, and storage devices, shall be physically protected against theft, unauthorized access, and damage.
- Physical access to critical IT infrastructure shall be restricted to authorized personnel only.

b. Disposal of IT Assets:
- Disposal of IT assets, including computers, hard drives, and storage media, shall follow secure procedures to prevent unauthorized data retrieval.
- Data stored on decommissioned or obsolete equipment shall be securely erased.

7. Incident Response and Reporting
a. Incident Reporting:
- Employees, volunteers, and contractors shall promptly report any suspected or actual security incidents, including unauthorized access, data breaches, malware infections, or any other IT security-related incidents, to the appropriate authority.

b. Incident Response:
- The HAAF shall maintain an incident response plan to address and mitigate the impact of security incidents.
- The incident response plan shall include procedures for containment, investigation, communication, recovery, and lessons learned.

c. Security Awareness and Training:
- The HAAF shall provide regular security awareness and training programs to educate employees, volunteers, and contractors about IT security best practices, procedures, and potential risks.

8. Policy Review

This policy shall be reviewed periodically to ensure its continued effectiveness and compliance with applicable laws, regulations, and industry standards. Any proposed changes to this policy shall be reviewed and approved by the appropriate HAAF authority.