Personal Data Breach Policy

Effective Date: 01 June 2023

1. Introduction
The Personal Data Breach Policy outlines the procedures to be followed in the event of a personal data breach within the Historic Army Aircraft Flight (HAAF). This policy aims to ensure a timely and effective response to data breaches, minimizing potential harm to individuals and complying with legal obligations regarding data protection and privacy.

2. Scope
This policy applies to all employees, volunteers, contractors, and individuals who handle personal data on behalf of the HAAF. It covers all types of personal data breaches, including accidental or unauthorized access, disclosure, loss, alteration, or destruction of personal data.

3. Definitions
a. Personal Data:
- Personal data refers to any information that relates to an identified or identifiable individual, as defined by applicable data protection laws and regulations.

b. Personal Data Breach:
- A personal data breach is a security incident that results in the accidental or unlawful destruction, loss, alteration, unauthorized disclosure, or access to personal data.

4. Personal Data Breach Response
a. Identification and Assessment:
- Upon becoming aware of a personal data breach, employees, volunteers, and contractors shall promptly report the breach to the designated Data Protection Officer (DPO) or other responsible authority within the HAAF.
- The DPO or responsible authority shall assess the breach to determine its scope, severity, potential risks to individuals, and legal obligations.

b. Containment and Mitigation:
- Immediate action shall be taken to contain and mitigate the impact of the breach.
- Appropriate measures may include suspending affected systems or accounts, disabling access, or implementing temporary security measures to prevent further unauthorized access or data loss.

c. Investigation and Documentation:
- A thorough investigation shall be conducted to determine the cause, extent, and consequences of the breach.
- The investigation findings, actions taken, and any remedial measures shall be documented in detail for future reference and accountability.

d. Notification and Communication:
- If required by applicable data protection laws and regulations, affected individuals and relevant supervisory authorities shall be notified of the breach in a timely manner.

- The notification shall provide clear and concise information about the nature of the breach, the potential risks involved, recommended actions for individuals, and contact information for further inquiries.

e. Remedial Actions and Preventive Measures:
- Following a personal data breach, appropriate remedial actions shall be taken to address vulnerabilities, prevent future breaches, and improve the overall security of personal data.
- Lessons learned from the breach shall be used to enhance data protection practices, revise security protocols, and provide additional training or awareness programs.

5. Record Keeping
a. Incident Register:
- The HAAF shall maintain a record of all personal data breaches, including details of the breach, actions taken, and outcomes.
- The incident register shall be securely stored and accessible to authorized personnel responsible for data protection and regulatory compliance.

b. Reporting Obligations:
- The HAAF shall fulfill its reporting obligations to relevant supervisory authorities, as required by applicable data protection laws and regulations.

6. Training and Awareness
- The HAAF shall provide regular training and awareness programs to employees, volunteers, and contractors on personal data protection, data breach response, and their responsibilities in ensuring the security of personal data.

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