Cyber Security Policy

Introduction:

The Historic Army Aircraft Flight (HAAF) is committed to ensuring the confidentiality, integrity, and availability of its information systems and data. As part of this commitment, HAAF has established a Cyber Security Policy to help protect its information systems and data from unauthorized access, use, disclosure, modification, or destruction. This policy applies to all volunteers, contractors, (and employees) of HAAF.

Policy:

1. Information Security Governance: The HAAF shall establish an Information Security Governance Framework that will ensure the effective management of cyber risks within the organization. This will include identifying and assessing risks, implementing controls, monitoring security, and reviewing security regularly.

2. Access Control: The HAAF shall implement appropriate access controls to ensure that only authorized individuals have access to its information systems and data. This includes controlling physical and logical access to its information systems and data, establishing strong authentication mechanisms, and ensuring that access rights are granted on a need-to-know basis.

3. Security Awareness and Training: The HAAF shall provide regular security awareness and training to all volunteers, contractors, and employees to ensure that they understand their roles and responsibilities in protecting the organization's information systems and data.

4. Incident Management: The HAAF shall establish an incident management process to ensure that security incidents are detected, reported, and responded to in a timely and appropriate manner. This includes defining roles and responsibilities, establishing reporting procedures, and implementing a response plan.

5. Data Protection: The HAAF shall implement appropriate measures to ensure the confidentiality, integrity, and availability of its data. This includes encryption of sensitive data, regular backups, and disaster recovery planning.

6. Physical Security: The HAAF shall implement appropriate physical security controls to protect its information systems and data. This includes controlling access to its physical facilities, securing equipment and media, and monitoring physical access.

7. Network Security: The HAAF shall implement appropriate network security controls to protect its information systems and data. This includes implementing firewalls, intrusion detection and prevention systems, and regularly monitoring network activity.

8. Third-Party Security: The HAAF shall ensure that all third-party suppliers and contractors are contractually obligated to comply with HAAF's Cyber Security Policy.

9. Compliance: The HAAF shall ensure compliance with all relevant legal, regulatory, and contractual requirements related to information security.

Summary

The HAAF takes the security of its information systems and data seriously and is committed to ensuring the confidentiality, integrity, and availability of its information systems and data. This Cyber Security Policy outlines the measures that the HAAF will implement to protect its information systems and data from unauthorized access, use, disclosure, modification, or destruction. All volunteers, contractors, and employees are required to comply with this policy, and any violation may result in disciplinary action, up to and including termination.