1. Purpose The purpose of this authorization level policy is to establish guidelines and standards for granting and managing access to sensitive information, systems, and resources of the Historic Aircraft Flight Trust (HAAF) charity. This policy aims to ensure the confidentiality, integrity, and availability of HAAF's assets while minimizing the risk of unauthorized access, data breaches, and misuse.
2. Scope This policy applies to all individuals, including employees, volunteers, contractors, and third-party service providers, who require access to HAAF's information systems, applications, databases, networks, and physical facilities.
3. Authorization Levels HAAF shall implement a hierarchical system of authorization levels based on the principle of least privilege. Each level grants specific access privileges based on the role and responsibilities of the authorized individuals. The following authorization levels are defined:
    a. Level 1: General Access
    - Individuals with Level 1 authorization are granted access to general information and non-sensitive resources required for their routine duties.
    - Access to Level 1 resources is granted to all employees and volunteers as necessary for their roles.

    b. Level 2: Sensitive Access
    - Individuals with Level 2 authorization have access to sensitive information and resources requiring additional protection.
    - Access to Level 2 resources is granted based on job responsibilities, need-to-know, and approval from the relevant department head or designated authority.

    c. Level 3: Restricted Access
    - Individuals with Level 3 authorization have access to highly sensitive information, critical systems, and resources.
    - Access to Level 3 resources is strictly controlled, granted on a need-to-know basis, and requires specific approval from the executive management or designated authority.
4. Access Provisioning The provisioning and management of access privileges shall follow the principle of separation of duties to prevent conflicts of interest and minimize the risk of unauthorized access. The following guidelines apply:
    a. Access requests must be submitted through HAAF's authorized access management system.
    b. Access requests must be approved by the appropriate supervisor or manager responsible for the individual's role.
    c. Access shall be provisioned based on job-related requirements and approved authorization levels.
    d. Access to sensitive systems or resources shall require additional approval from the IT department or designated authority.

e. Access provisioning and deprovisioning shall be completed in a timely manner based on personnel changes or role transitions.

5. Monitoring and Auditing HAAF shall implement monitoring and auditing mechanisms to ensure compliance with this authorization level policy. The following measures shall be taken:

   a. Regular review of user access rights to ensure alignment with job roles and responsibilities. b. Monitoring of access logs and audit trails to detect and investigate any unauthorized access attempts. c. Periodic security assessments and reviews to identify potential vulnerabilities and ensure compliance with relevant regulations and best practices.

6. Policy Compliance Failure to comply with this authorization level policy may result in disciplinary action, up to and including termination of employment or volunteer status, and may also be subject to legal consequences as applicable.

7. Policy Review This policy shall be reviewed and updated periodically to reflect changes in technology, business requirements, and regulatory frameworks. Any proposed changes to this policy shall be reviewed and approved by the executive management or designated authority.