Aerosprim Security Clearance & Confidentiality Policy

Effective Date: August 17, 2025

AeroSprim conducts advanced aerospace projects, and certain activities involve sensitive technical data and proprietary information. This policy governs access, handling, and protection of such information to ensure the safety, integrity, and confidentiality of all club projects.

1. Purpose

The purpose of this policy is to:

- Protect confidential project data, designs, and research.
- Define member responsibilities regarding sensitive information.
- Establish access levels and clearance procedures.
- Ensure compliance with applicable laws and ethical standards.

2. Scope

This policy applies to:

- All AeroSprim members, volunteers, and collaborators.
- All club projects, documents, designs, digital files, and communications.
- Physical and digital spaces where sensitive activities or information are stored.

3. Classification of Information

All AeroSprim information is classified into the following categories:

1. **Public Information:** Non-sensitive content that can be shared freely, such as event announcements, public-facing project summaries, or promotional material.
2. **Internal Information:** Club-related data that should be shared only among members, such as internal communications, meeting notes, or basic project plans.
3. **Confidential Information:** Sensitive project designs, experimental data, proprietary research, or any information that could compromise safety, security, or intellectual property if disclosed.

4. Access & Clearance Levels

- **General Member Access:** Limited to public and internal information. Members may view project summaries and attend standard workshops.
- **Project Team Access:** Granted to members actively participating in specific projects. These members may access internal and confidential information relevant to their project.
- **Leadership Access:** Club leaders and designated officers have full access to all project and operational information.

Access to confidential information requires:

- Completion of a security briefing.
- Signing a Non-Disclosure Agreement (NDA) specific to the project.
- Adherence to all handling and storage protocols.

5. Handling and Protection of Confidential Information

Members must:

- Store digital files in approved, secure storage (e.g., password-protected cloud folders).
- Not share confidential information outside the club or with unauthorized members.
- Report any suspected security breaches immediately to club leadership.
- Properly dispose of sensitive physical documents (shredding or secure storage).
- Avoid discussing sensitive project details in public areas or online.

6. Use of Personal Devices and Communications

- Personal devices may be used for project work only if approved by the project team leader.
- Sensitive data must not be transmitted over unsecured networks.
- Club email and collaboration tools should be used for internal communications instead of personal messaging apps.

7. Violations and Consequences

Violations of this policy, including unauthorized disclosure of confidential information, may result in:

- Revocation of access or membership.
- Removal from specific projects or leadership roles.
- Legal action if the breach involves intellectual property or violates applicable laws.

8. Policy Updates

AeroSprim may update this policy as needed. All members will be notified of changes, and continued participation indicates acceptance of the updated security protocols.

9. Contact

For questions or reports of security incidents, email aerosprim@gmail.com or contact club leadership directly.