#### Document Control Information:

###### **Document ID:** A3-SIH-01

###### **Version:** 1.0

###### **Date:** 07/10/2024

#### Introduction

###### The Sensitive Information Handling Protocol is designed to ensure that all forms of sensitive data managed by Arch Angel Agency are handled with the highest level of security and confidentiality. This document provides comprehensive guidelines for securing sensitive information, preventing unauthorized access, and ensuring data integrity. Adherence to these protocols is mandatory for all personnel.

### Objective

###### To establish standardized practices for handling, storing, and transmitting sensitive information within Arch Angel Agency, thus protecting our assets from unauthorized access, disclosure, alteration, and destruction.

#### Scope

###### This protocol applies to all employees, contractors, and third-party agents of Arch Angel Agency who have access to sensitive information across all platforms and media.

##### Protocols Overview

###### The following eight protocols have been established to guide the handling of sensitive information within the agency

###### **Protocol 1: Data Classification and Control**

###### Define categories of sensitivity and corresponding security measures.

###### **Protocol 2: Secure Access Controls**

###### Implement access restrictions based on roles and responsibilities.

###### **Protocol 3: Encryption and Data Protection**

###### Encrypt sensitive data both in transit and at rest.

###### **Protocol 4: Incident Response and Management**

###### Establish procedures for responding to security breaches.

###### **Protocol 5: Physical Security Measures**

###### Secure physical access to information storage areas.

###### **Protocol 6: Audit and Compliance**

###### Regular audits to ensure compliance with these protocols.

###### **Protocol 7: Employee Training and Awareness**

###### Ongoing security training for all agency personnel.

###### **Protocol 8: Third-Party Security Requirements**

###### Enforce security standards for all external partners and contractors.

## Protocol 1: Data Classification and Control

**Objective:** To define and classify data based on its level of sensitivity and criticality, ensuring that appropriate security measures are implemented corresponding to the level of data sensitivity.

**Classification Levels:**

• **Public:** Information intended for public disclosure. No harm is expected if accessed by unauthorized parties.

• **Internal Use Only:** Information restricted to agency personnel. Disclosure or unauthorized access could impact the agency’s operations or reputation mildly.

• **Confidential:** Information that could cause damage to the agency or its clients if disclosed. Access is tightly controlled and monitored.

• **Top Secret:** Information that could cause severe damage if disclosed. This includes data under legal protection, sensitive personal information, and high-value operational intelligence.

**Controls:**

• Regular audits to ensure proper classification.

• Labeling of all documents and digital files according to their classification.

• Strict handling and dissemination protocols based on classification.

## Protocol 2: Secure Access Controls

**Objective:** To prevent unauthorized access to sensitive information by implementing stringent access controls based on roles and responsibilities within the agency.

**Access Control Measures:**

• **Role-Based Access Control (RBAC):** Access rights are granted according to the roles within the agency, ensuring that personnel can only access information necessary for their job functions.

• **Authentication Mechanisms:** Use of multi-factor authentication (MFA) across all systems handling sensitive data.

• **Periodic Access Reviews:** Regular reviews of access rights to ensure they are appropriate and that no unnecessary access is granted.

## Protocol 3: Encryption and Data Protection

**Objective:** To safeguard sensitive data from unauthorized access or breaches by encrypting data both in transit and at rest.

**Encryption Practices:**

• **Data at Rest:** Implement AES-256 encryption for all stored data classified as Confidential or higher.

• **Data in Transit:** Use TLS 1.2 or higher for all data transmitted over public networks.

• **Key Management:** Use secure key management practices to generate, store, and retire encryption keys.

## Protocol 4: Incident Response and Management

**Objective:** To establish a robust framework for responding to security incidents to minimize damage, recover from breaches, and prevent future occurrences.

**Incident Response Plan:**

• **Detection and Reporting:** Mechanisms to detect and report potential security incidents immediately.

• **Assessment and Analysis:** Procedures to assess and analyze the impact and scope of the incident.

• **Containment and Eradication:** Steps to contain the incident and eradicate the cause.

• **Recovery and Review:** Processes to recover systems to normal operation and review the incident to improve future response efforts.

**Training:** Regular training and simulations for the incident response team to ensure preparedness.

## Protocol 5: Physical Security Measures

**Objective:** To secure physical access to information storage areas to prevent unauthorized access, damage, or theft of physical and digital information assets.

**Security Measures:**

• **Controlled Access:** Implement key card access systems to restrict and monitor entry into sensitive areas.

• **Surveillance Systems:** Deploy CCTV surveillance across all sensitive areas to deter unauthorized access and record all activities for review if needed.

• **Secure Storage:** Utilize safes and locked cabinets for storing highly sensitive physical documents and media.

• **Visitor Management:** Establish a strict visitor protocol that includes escorts and logbooks to maintain a record of all non-employee access to sensitive areas.

## Protocol 6: Audit and Compliance

**Objective:** To ensure ongoing compliance with all established security protocols and guidelines through regular audits and reviews.

**Audit Practices:**

• **Internal Audits:** Conduct scheduled and random audits to assess the adherence to security protocols.

• **External Audits:** Engage third-party security firms to conduct annual audits, providing an unbiased review of security practices.

• **Remediation Plans:** Develop and implement remediation plans for any non-compliance found during audits.

• **Compliance Reporting:** Regularly report compliance status to management and relevant oversight bodies.

## Protocol 7: Employee Training and Awareness

**Objective:** To maintain a high level of security awareness and preparedness among all agency personnel through continuous training and education.

**Training Programs:**

• **New Employee Security Orientation:** Introduce new hires to the agency’s security protocols and expectations.

• **Ongoing Training Sessions:** Conduct regular training sessions to refresh security practices and introduce new security measures.

• **Simulated Security Exercises:** Perform simulated security breach exercises to prepare employees for actual security incidents.

• **Awareness Campaigns:** Implement ongoing security awareness campaigns to keep security at the forefront of agency operations.

## Protocol 8: Third-Party Security Requirements

**Objective:** To ensure that all external partners and contractors adhere to the same stringent security standards as internal operations to protect shared sensitive information.

**Security Requirements:**

• **Security Assessments:** Evaluate the security measures of potential partners before initiating any formal relationship.

• **Contracts and Agreements:** Include strict security clauses in contracts with third parties that outline the expectations and responsibilities related to data security.

• **Regular Reviews:** Periodically review third-party security practices and compliance through audits and meetings.

• **Incident Response Coordination:** Establish protocols for coordinating incident response efforts with third-party partners to ensure quick and effective action in case of a breach involving shared information.

# Final Protocol

## Amendments, Updates, and Governance

**Objective:** To ensure that the Sensitive Information Handling Protocol remains current and effective in addressing emerging security challenges and changes in regulatory requirements.

### Protocol Management:

• **Review and Updates:** This document shall be reviewed at least annually or as needed to respond to significant changes in technology, business operations, or security threats. The designated security team is responsible for initiating reviews.

• **Amendment Procedures:** Amendments to this protocol must be proposed in writing, including a detailed description of the proposed changes and justification for the amendment. All amendments must be approved by the Agency’s Director of Security and Compliance.

• **Document Control:** Maintain a version-controlled system to track all changes made to this protocol. Each version should be archived for audit purposes, and only the most current version shall be actively distributed and implemented.

• **Stakeholder Involvement:** Involve key stakeholders in the review process, including IT, legal, human resources, and operational departments, to ensure that all perspectives are considered in maintaining comprehensive security practices.

#### Compliance and Enforcement:

• **Obligatory Compliance:** Adherence to this protocol is mandatory for all employees, contractors, and third-party partners. Violations of the protocol can result in disciplinary action, up to and including termination of employment or contractual relationships.

• **Enforcement Mechanisms:** Regular compliance checks and enforcement measures will be conducted to ensure that all personnel and partners adhere to the prescribed security practices. Non-compliance will be addressed promptly to mitigate any potential security risks.

• **Reporting Violations:** Employees are encouraged to report any observed violations or security weaknesses through the established whistleblowing channels. Confidentiality of the reporting individual will be maintained to protect them from retaliation.

# Final Protocol

## Training, Awareness and Documentation Availability

### Training and Awareness:

• **Protocol Education:** Upon protocol amendment, relevant training sessions will be conducted to familiarize all agency personnel with the changes. Continuous education efforts will be made to reinforce the importance of protocol compliance.

• **Awareness Campaigns:** Regular campaigns will be conducted to keep security awareness high and ensure that the protocols are understood and followed by everyone in the agency.

#### Document Availability:

• **Accessibility:** This document will be readily accessible to all employees through the agency’s internal document management system. Physical copies may be provided in critical areas as necessary.

• **Confidentiality of the Protocol:** While this protocol is intended for internal use, certain sections may be shared with external auditors or regulatory bodies as required for compliance verification.

# Zero Protocol

### [Creative Commons Zero (CC0)](https://creativecommons.org/public-domain/cc0/) Protocol for Public Domain Declaration

##### Introduction

This protocol outlines the procedures and criteria for placing agency-created intellectual property (IP) under the Creative Commons Zero (CC0) waiver, effectively dedicating it to the public domain. This action removes restrictions on the use of the IP, allowing anyone to use, modify, and distribute the content without any need for attribution.

### Objective

To foster an open knowledge environment by making select agency-created intellectual property freely available to the public and other stakeholders, thereby supporting innovation and transparency.

#### Scope

This protocol applies to all digital and physical works created by employees of Arch Angel Agency, including but not limited to documents, software, databases, educational materials, and artworks.

##### Criteria for CC0 Designation

1. **Eligibility Assessment:** Determine if the IP is solely owned by the agency and free from any third-party copyrights.
2. **Value and Impact Review:** Assess the potential value and impact of releasing the IP under CC0, considering the agency’s strategic objectives and public benefits.
3. **Legal Clearance:** Conduct a thorough legal review to ensure that dedicating the IP to the public domain does not conflict with any existing laws, regulations, or contractual obligations.

# Zero Protocol

### [Creative Commons Zero (CC0)](https://creativecommons.org/public-domain/cc0/) Protocol for Public Domain Declaration

#### Protocol for Declaration

1. **Initiation:**
   * Any department within the agency can propose IP for CC0 designation through a formal proposal outlining the IP’s description and justification for its release.
2. **Review and Approval:**
   * The proposal will be reviewed by a designated Public Domain Review Committee, which includes members from legal, management, and relevant technical departments. The process should be democratic.
3. **Documentation:**
   * Upon approval, document the details of the IP and the decision for CC0 designation in the agency’s IP registry.
4. **Declaration:**
   * Apply the Creative Commons CC0 legal waiver to the IP. This involves completing the CC0 declaration form available from Creative Commons and attaching it to the IP.
5. **Public Announcement:**
   * Publicly announce the CC0 dedication through the agency’s official communication channels to ensure visibility and access.

##### Responsibilities

* **Legal Department:**
  + To provide legal oversight and ensure compliance with all relevant laws and regulations.
* **Communications Department:**
  + To handle public announcements and dissemination of CC0-dedicated IP.
* **IT Department:**
  + To manage the technical aspects of documenting and applying the CC0 waiver to digital products.

### Amendments and Updates

###### This protocol will be reviewed annually or as needed to adapt to changes in copyright law, agency policy, or public domain practices.