ACA WSO Information Security Policy

This policy establishes the information security requirements applicable to ACA WSO **key volunteers**.

1. Purpose The purpose of this policy is to establish a framework for ensuring the confidentiality, integrity, and availability of information assets within ACA WSO. This policy defines information security objectives and sets the foundation for related standards and procedures.

2. Scope This policy applies to all key volunteers, who have access to ACA WSO's information assets. It covers all systems, networks, applications, and data owned, managed, or processed by the organization. For purposes of this policy, *key volunteers* are defined as volunteers who have access to ACA WSO's information assets.

3. Information Security Objectives ACA WSO is committed to achieving the following information security objectives:

1. **Confidentiality:** Ensure that information is accessible only to authorized individuals and protected from unauthorized disclosure.
2. **Integrity:** Safeguard the accuracy and reliability of information to prevent unauthorized modification, deletion, or corruption.
3. **Availability:** Ensure that critical information and systems remain accessible and functional when required.
4. **Regulatory Compliance:** Adhere to applicable laws, regulations, and industry standards governing information security and data protection.
5. **Risk Management:** Identify, assess, and mitigate risks related to information security.
6. **Security Awareness:** Promote a culture of security awareness through regular training and education programs.
7. **Incident Response:** Establish procedures to detect, respond to, and recover from security incidents effectively.
8. **Continuous Improvement:** Continuously enhance security measures through audits, reviews, and adoption of industry best practices.

4. Compliance Responsibilities

- **General Manager** is responsible for ensuring that information security policies and practices align with business objectives and regulatory requirements.
- **IT Manager** is responsible for overseeing the implementation and enforcement of this policy.
- **IT Special Workers** are responsible for monitoring threats, deploying security controls, and responding to incidents.
- **Key Volunteers** must comply with all information security policies, standards, and procedures.

5. Supporting Standards and Procedures To implement this policy, ACA WSO has developed supporting standards and procedures, including but not limited to:

- Access Control Policy (see addendum A)
- Incident Response Plan (see Addendum B)
- Security Awareness Training Procedures (see Addendum C)

6. Policy Compliance

Compliance to this policy applies to all key volunteers who have access to ACA WSO's information assets.

Non-compliance with this policy may result in disciplinary action, including termination of volunteer service relationship, legal action, or other penalties as applicable. Compliance audits and security assessments will be conducted periodically to ensure adherence to this policy.

7. Review and Updates This policy will be reviewed at least annually and updated as necessary to reflect changes in regulations, business needs, and emerging security threats.

8. Contact Information For any questions regarding this policy, please contact the IT Manager (itmanager@acawso.org)

Approval and Acknowledgment By signing below, I acknowledge that I have read and understand this Information Security Policy and agree to comply with its requirements.

Name: _____

Position: _____

Date: _____

Signature:_____

Appendix A

Access Control Policy

ACA WSO
Version: 1.0

1. Purpose

The purpose of this policy is to establish guidelines for controlling access to ACA WSO's information systems, networks, and data. This policy ensures that only authorized individuals have access to company resources, minimizing security risks and protecting sensitive business information.

2. Scope

This policy applies to all ACA WSO key volunteers who have access to company systems, data, or networks.

3. Roles & Responsibilities

3.1 General Manager (GM)

- Approves all access control policies.
- Reviews high-level access permissions for IT staff and business-critical applications.
- Ensures IT security compliance.

3.2 IT Manager

- Oversees the implementation and enforcement of access control policies.
- Reviews and approves user access requests.
- Conducts periodic access audits.

3.3 IT Administrator

- Implements access controls and maintains user accounts.
- Monitors systems for unauthorized activities.
- Ensures proper user authentication and authorization.

3.4 Key Volunteers

- Must follow access control procedures.
- Responsible for securing their credentials.
- Report any unauthorized access or security incidents to the IT Manager.
- Ensure that information is accessible only to authorized individuals and protected from unauthorized disclosure.

4. Access Control Principles

4.1 Least Privilege

Users will be granted the minimum level of access required to perform their function.

4.2 Role-Based Access Control (RBAC)

Access is assigned to key volunteers based on job roles:

- **Board Chair -** Full system access in the event the General Manager and IT Manager are unable to perform their responsibilities.
- **Other Key Volunteers** – Limited access to business applications and data sources relevant to their roles.

4.3 Authentication & Password Policy

- All users must employ **strong passwords** (minimum 8 characters, mix of uppercase, lowercase, numbers, and symbols).
- Multi-Factor Authentication (MFA) is required for administrative accounts.
- Users must not share passwords with others
- Passwords should be changed annually

4.4 Account Management

- New user access requests must be approved by the **IT Manager**.
- Access is revoked immediately upon termination of the volunteer service relationship.
- Accounts inactive for **90 days** will be disabled.
- Unauthorized access attempts must be reported to the **IT Manager**.

5. Access Review & Audits

- Access permissions will be reviewed **annually** by the **IT Manager.**
- Annual security audits will be conducted to verify compliance.

6. Enforcement & Violations

- Key volunteers violating this policy may face termination of service or revocation of access
- Security incidents must be reported immediately to the **IT Manager**.

7. Policy Review

This policy will be reviewed annually and updated as needed.

Appendix B

IT Incident Response Plan

1. Introduction

This IT Incident Response Plan is designed to help ACA WSO effectively detect, respond to, and recover from IT security incidents while minimizing business disruption and data loss. This plan is tailored for a small organization, such as WSO, with an IT team consisting of an **IT Manager** and an **IT Administrator**, both reporting to the **General Manager**.

2. Roles and Responsibilities

2.1 General Manager (GM)

- Provides executive oversight and final decision-making authority on major incidents while keeping the Board informed.
- Coordinates with external stakeholders (e.g., law enforcement, vendors, legal team) as needed.
- Approves communications to employees, volunteers and/or the Fellowship regarding incidents.

2.2 IT Manager

- Leads the incident response efforts.
- Assesses and classifies the severity of incidents.
- Directs the IT Administrator in containment, mitigation, and recovery actions.
- Reports incidents and response progress to the General Manager.
- In conjunction with the General Manager ensures the Board is kept up-to-date on major incidents and mitigation efforts.

2.3 IT Manager/IT Administrator

- Implements technical solutions to contain, eradicate, and recover from incidents.
- Conducts initial investigations, logs activities, and gathers forensic evidence.
- Maintains IT systems, backups, and security controls to prevent future incidents.

3. Incident Response Phases

3.1 Preparation

- Maintain up-to-date antivirus, firewalls, and intrusion detection systems.

- Provide regular security awareness and incident report training to employees and contractors.
- Ensure regular data backups and testing of disaster recovery plans.
- Keep an updated inventory of IT assets and access control lists.
- Conduct periodic tabletop exercises or other incident response testing, as appropriate.
- Review and update this Incident Response Plan annually and following significant incidents or material changes to ACA WSO's technology or operations.

3.2 Detection and Analysis

- Monitor IT systems for anomalies or suspicious activity using security tools and log analysis.
- Identify and verify potential security incidents.
- Assess the scope, impact, and severity of the incident.
- Classify incidents based on severity:
    - **Low:** Minor system disruptions, failed login attempts.
    - **Medium:** Malware infections, unauthorized access attempts.
    - **High:** Data breaches, ransomware, system-wide outages.
- IT Manager determines if the incident requires escalation to the General Manager.

3.3 Containment

- Short-term containment: Isolate affected systems (e.g., disconnect from the network, disable compromised accounts).
- Long-term containment: Apply security patches, change passwords, reconfigure firewall rules.
- Document containment actions and ensure minimal impact on business operations.

3.4 Eradication

- Identify root cause and remove malicious files, unauthorized accounts, or exploited vulnerabilities.
- Scan affected systems with updated security tools.
- Patch software and apply additional security measures.

3.5 Recovery

- Restore systems from verified backups if necessary.
- Monitor systems closely for any signs of lingering threats.
- Validate system functionality and confirm that business operations are fully restored.

3.6 Post-Incident Review and Documentation

- Conduct a debrief meeting led by the IT Manager.
- Document the timeline of events, actions taken, and key takeaways.
- Update security policies and incident response procedures based on findings.
- Provide recommendations to the General Manager for future improvements.

4. Communication and Escalation Procedures

- **Internal Communication:**
  - All IT incidents must be reported to the IT Manager immediately.
  - The IT Manager escalates critical incidents to the General Manager.

- **External Communication:**
  - The General Manager determines if law enforcement, legal counsel, or affected members of the Fellowship need to be notified.
  - No volunteer should communicate about security incidents publicly or on social media without authorization.

Appendix C

Security Awareness Training Procedures

1. Purpose

The purpose of this document is to establish procedures for security awareness training at ACAWSO. All key volunteers (as identified by the IT Manager and/or the General Manager) are required to complete cybersecurity training to ensure the protection of company assets, data, and systems from cyber threats.

2. Scope

This procedure applies to all key volunteers who have access to company systems, networks, or data.

3. Responsibilities

3.1 Management

- Selects a cybersecurity training vendor to provide comprehensive training.
- Ensures that key volunteers have access to the training resources.
- Monitors and enforces compliance with training requirements.
- Evaluates the effectiveness of the training program on an annual basis.

3.2 Key Volunteers

- Complete the required cybersecurity training within the designated timeframe.
- Apply learned cybersecurity best practices in daily work activities.
- Report any security incidents or suspicious activities to the IT Manager.

3.3 IT Team

- Manages the cybersecurity training program in collaboration with the selected vendor.
- Tracks and reports key volunteer training completion status.
- Provides additional guidance or support to employees regarding cybersecurity best practices.

4. Training Requirements

4.1 Mandatory Training

- All key volunteers must complete the cybersecurity training provided by the vendor selected by ACAWSO management.
- Training must be completed within 60 days of beginning a role as a key volunteer.

4.2 Training Delivery

- Training will be delivered via an online learning management system (LMS) provided by the vendor.
- Key volunteers may be required to complete quizzes or assessments to demonstrate understanding.
- Additional in-person or virtual workshops may be scheduled as needed.

5. Compliance and Monitoring

- Key volunteers must provide proof of training completion through the LMS.
- The IT Team will generate compliance reports and share them with management.
- Failure to complete training within the specified timeframe may result in restricted system access.

6. Review and Updates

- This procedure will be reviewed annually by ACA WSO management and the IT Security Team to ensure alignment with evolving cybersecurity threats and best practices.
- Updates will be communicated to all key volunteers as necessary.