AR Workflow

AR WORKFLOW WEB APP SECURITY POLICY

1. Introduction

This policy is a foundational framework detailing the protective measures adopted by AR Workflow to safeguard user data, ensure system reliability, and uphold the standards compliance requirements.

2. Scope

This policy spans across all team members, contractors, systems, and external vendors associated with the AR Workflow Web App, encompassing both the application's data and operational infrastructure.

3. Objectives

- **Confidentiality:** Guard user data from unauthorized disclosure.
- **Integrity:** Maintain the accuracy and consistency of data and system operations.
- **Availability**: Ensure uninterrupted access to the system and data.
- **Continuous Improvement:** Regularly revise strategies to address emerging threats and vulnerabilities.

4. Security Awareness and Training

- **Orientation:** New hires receive immediate training about security protocols.
- **Refresher Courses:** Annual or bi-annual retraining to update staff on new threats and defense mechanisms.
- **Evaluation:** Post-training evaluations to confirm understanding and retention.

5. Access Control

- **Role-Based Access:** Clearly defined roles dictating permitted actions for users.
- **Principle of Least Privilege:** Users granted the minimal level of access required to perform their duties.
- **Authentication:** MFA is mandatory for critical areas and sensitive data access.
- **Audit Trails:** Comprehensive logs of access to facilitate backtracking in case of breaches.

6. Data Encryption

- **End-to-End Encryption:** Data encrypted both in transit (e.g., TLS) and at rest (e.g., AES).
- **Key Management:** Scheduled encryption key rotations, secure storage, and restricted access to keys.

7. Network Security

- **Firewalls:** Deployed to filter incoming/outgoing traffic, blocking unauthorized access.
- **Intrusion Detection:** Real-time alerts for any suspicious activity.
- **Regular Scans:** Frequent vulnerability assessments using updated tools to pinpoint weak spots.

8. Data Backup and Recovery

- **Backup Scheduling:** Daily, weekly, and monthly backup routines.
- **Off-Site Storage:** Backups stored in geographically separate locations to minimize data loss risks.

- **Redundancy:** Multiple backup versions maintained to counteract data corruption.

9. Incident Response
   - **Response Team:** Dedicated team on standby for security incidents.
   - **Procedures:** Step-by-step guide, from identification to resolution and post-incident analysis.
   - **Communication:** Procedures for notifying affected parties, including users and regulatory bodies.

10. Vendor Management
    - **Due Diligence:** Comprehensive assessments of vendor security policies before engagement.
    - **Continuous Monitoring:** Regular review of vendor compliance and potential vulnerabilities.
    - **Contractual Obligations:** Explicit data protection clauses in contracts.

11. Patch Management
    - **Monitoring:** Track updates from software providers for relevant systems.
    - **Deployment:** Staging environment tests before applying patches.
    - **Documentation:** Record all applied patches with date, time, and outcomes.

12. Physical Security
    - **Facility Protection:** Biometric and card-based entry systems, 24/7 guards, and alarm systems.
    - **Visitor Logs:** Maintain and review records of all non-employee facility access.
    - **Environmental Controls:** Redundant power supplies, fire suppression systems, and HVAC to protect equipment.

13. End-point Security
    - **Device Management:** Control over devices accessing the web app through Mobile Device Management (MDM) solutions.
    - **Remote Wipe:** Capability to erase data from lost or stolen devices.
    - **Patch Updates:** Devices required to be updated to the latest security patches.

14. Policy Enforcement and Penalties
    - **Monitoring:** Continuous observation tools to detect policy violations.
    - **Penalty Framework:** Graduated penalties, from warnings to potential employment termination.
    - **Review & Update:** Regular examination of enforcement mechanisms for efficacy.

15. Policy Review
    - **Annual Review:** Full review of the policy, analyzing outcomes and emerging threats.
    - **Stakeholder Input:** Taking feedback from users, IT staff, and management to refine the policy.
    - **Regulatory Alignment:** Adjustments to remain compliant with evolving regulatory requirements.