



INTERACTIVE PUBLIC OUTREACH

PUBLIC WHITE PAPER

Security, Privacy, and Data Protection

A clear overview for departments, procurement teams, public-safety leaders, and community stakeholders

Version 1.1 | September 15, 2026 | A2C3 Outreach LLC

A2C3 Interactive Public Outreach delivers browser-based public education and privacy-minimized aggregate reporting without requiring public participant accounts.

This paper explains the platform's verified safeguards and current assurance status. It intentionally excludes credentials, private identifiers, security configurations, endpoint inventories, raw logs, control thresholds that could aid abuse, and detailed attack or bypass information.

Current status

A2C3 has a meaningful pre-launch security foundation. Operational and independent-assurance work remains before paid municipal production. A2C3 does not claim independent certification or completed penetration testing.

Guiding principles

- Collect less information from public participants.
- Keep each department's access and reporting inside the correct workspace.
- Enforce privileged permissions on the server.
- Use aggregate reporting and suppression to reduce small-group privacy risk.
- Maintain recoverable releases and backups while communicating limitations honestly.

**01 | PRIVACY**

Data practices designed for public trust

No public participant account required

Public educational programs do not require a name, email address, telephone number, street address, school, age, or personal profile. The experience is designed around program use and aggregate outcomes rather than named participant histories.

Information categories

Category	Purpose	Public treatment
Program content	Deliver education and approved department branding	Public after release approval
Aggregate analytics	Measure reach, completion, topics, and campaigns	Department-scoped and privacy-limited
Short-lived technical signals	Maintain session integrity and deter abuse	Purpose-limited and time-bounded
Administrative records	Manage authorized staff, releases, reports, and support	Protected workspace access

Analytics privacy

Program events are validated and associated with the appropriate department, program, and campaign. Reporting is aggregated, and small sample groups are suppressed or restricted so ordinary reports do not expose individual participants.

Purpose-based retention

Different information follows different lifecycles. Short-lived technical data expires sooner than aggregate reporting data. Customer agreements, public-record obligations, legal holds, and documented offboarding requirements may affect a specific retention decision.

Public privacy boundary

The platform is not designed to create named participant histories. Departments should avoid using campaigns or program content to solicit sensitive personal information unless a separately reviewed and lawful process has been established.

**02 | SECURITY**

Protected access and application safeguards

Access control and department separation

A2C3 separates public participation, department administration, and platform-owner administration. Protected workspaces use authenticated access and role-based permissions. Server-side controls determine the organization and functions an authenticated user may access; publicly supplied identifiers do not authorize access to another department's information.

- Department administrators manage authorized users and organization settings within their assigned workspace.
- Editors perform approved content and operational tasks without account-management authority.
- Viewers receive read-only access to assigned reporting and program information.
- Administrative sessions can be revoked, and material account changes are recorded for review.
- Published branding is separated from drafts and private review material.

Safeguard summary

Control area	Public summary
Encrypted connections	Web traffic is served over HTTPS with managed certificate handling.
Browser protections	Security policies restrict framing, unsafe content handling, and unnecessary capabilities.
Authentication	Protected workspaces use secure session, throttling, recovery, and credential controls.
Authorization	Protected actions use server-side role and department checks.
Input and uploads	Requests and approved asset uploads are validated and bounded before processing.
Secrets	Sensitive configuration stays outside public content and routine customer exports.
Audit evidence	Administrative, authentication, release, delivery, and export activity is recorded.



03 | ASSURANCE

Continuity, response, and readiness

Continuity and recovery

A2C3 maintains versioned application releases and checksummed operational exports. Recovery copies use separate cloud and encrypted physical processes so a single platform failure does not represent the only copy. Restoration is intended to occur in an isolated environment first, followed by integrity, record-count, asset, access, and functional checks.

- Backup packages use integrity checks to detect unexpected changes.
- Routine exports exclude authentication secrets and restricted credential material.
- Recovery procedures include access review and credential reset before return to service.
- A full operational restoration drill remains part of pre-launch readiness.

Monitoring and incident response

Service health checks, protected logs, administrative audit records, authentication events, analytics-integrity records, delivery records, and backup evidence support operational review. The response framework covers detection, containment, evidence preservation, assessment, notification analysis, remediation, recovery, and post-incident review.

Notification obligations depend on the affected information, applicable law, and the governing customer agreement. This paper does not create a universal notification deadline or contractual service level.

Shared responsibility

A2C3 is responsible for platform safeguards, department scoping, protected administration, privacy-minimized reporting, backup evidence, and accurate control documentation. Departments remain responsible for authorizing staff, protecting devices and credentials, reviewing account changes, supplying lawful content, and interpreting aggregate reports in context.

Current readiness priorities

- Enforce and verify multi-factor authentication before real department administrators receive production access.
- Complete a full isolated backup restoration drill.
- Complete independent authenticated web and API penetration testing before a paid municipal pilot.
- Complete offboarding, incident-response, accessibility, legal, insurance, and procurement evidence.

Assurance statement

A2C3 is in pre-launch evaluation. Internal technical reviews and automated checks are not independent assurance. A2C3 has not completed an independent authenticated penetration test and does not claim SOC 2 or ISO 27001 certification, FedRAMP authorization, or universal compliance with sector-specific frameworks. Provider certifications should not be interpreted as certifications of A2C3 itself.

Security information requests

Departments may request a controlled security and procurement review through a2c3outreach.com. Additional evidence may be shared with authorized reviewers when appropriate; restricted implementation details, credentials, private records, and raw security evidence are not distributed through this public paper. This paper is informational, does not amend a customer agreement, and is replaced when material controls or assurance status change.