

CITY OF ANNISTON, ALABAMA

Public Relations Department Policy Manual

A unified City standard for communications, social media, artificial intelligence governance, digital accessibility, privacy, online documents, and film-production coordination

Policy owner: Public Relations / Communications Department
City Hall | 1129 Noble Street | Anniston, Alabama 36201
AnnistonAL.gov

Policy Administration

Manual title	Public Relations Department Policy Manual
Policy owner	Public Relations / Communications Department
Executive oversight	City Manager
Coverage	Official communications, social media, AI-assisted work, public-facing digital content and documents, privacy and personal information, and film-production coordination
Applies to	Departments, boards, commissions, employees, officials, interns, volunteers, contractors, vendors, and authorized users acting for the City
Administration	Public Relations Director, in coordination with Information Technology, the City Clerk, Human Resources, Purchasing, Risk Management, department heads, and the City Attorney
Review cycle	At least annually and after a material change in law, technology, platform operations, security risk, or City procedure

Unified manual

This book consolidates the City's public-relations operating standards into one policy system. It is written for day-to-day use and should be read together with adopted law, personnel rules, records schedules, cybersecurity requirements, and emergency procedures.

No implied legislative action

This administrative manual does not represent that City Council has adopted a measure unless the Clerk's official records show adoption. Ordinance-dependent fees, penalties, or regulatory requirements are not created by this manual.

Contents

Policy Administration	2
Department Foundations	7
1 Purpose	8
2 Scope	8
3 Communications Governance	9
3.1 Department Administration and Standard Operating Procedures	9
4 Department Request and Approval Workflow	10
5 Temporary Modified Duty	10
Social Media Policy	11
1. Purpose and Policy Statement	11
2. Scope	11
3. Definitions	12
4. Governance and Responsibility	12
5. Account Approval, Ownership, and Closure	13
5.1 Approval before creation	13
5.2 City ownership and account inventory	13
5.3 Inactive or closing accounts	13
6. Access Control and Cybersecurity	13
7. Content Standards and Approval	14
7.1 Municipal purpose and voice	14
7.2 Accuracy, sourcing, and corrections	14
7.3 Approval matrix	15
7.4 Privacy, dignity, copyright, and releases	15
7.5 Links, likes, shares, follows, and endorsements	15
8. Accessibility and Inclusive Communication	15
9. Artificial Intelligence, Automation, and Synthetic Media	16
10. Public Comments and Moderation	17
10.1 Forum designation and notice	17
10.2 Viewpoint-neutral rule	17

10.3 Content eligible for restriction	17
10.4 Moderation procedure	17
10.5 Blocking, muting, and comment closure	18
10.6 Appeals	18
11. Records, Retention, and Public Records Requests	18
12. Direct Messages, Service Requests, and Customer Care	19
13. Emergency and Crisis Communications	19
14. Employees, Officials, and Personal Accounts	20
14.1 Personal expression	20
14.2 Keeping personal and official activity distinct	20
14.3 Elected and appointed officials	20
15. Elections, Campaigns, and Political Activity	20
16. Training, Monitoring, and Enforcement	21
17. Administration, Exceptions, and Review	21
Public-Facing Social Media Comment Guidelines	22
Administrator Checklists and Moderation Record	24
B.1 Before publishing	24
B.2 Before moderating	24
B.3 Moderation record fields	25
Authorized User Acknowledgment	26
Legal and Administrative References	27
Artificial Intelligence Policy and Governance	29
18. Purpose, Scope, and Core Rule	29
19. Definitions	29
20. Responsible AI Principles	29
21. Governance and Responsibility	30
22. Risk Classification	30
23. Allowed, Restricted, and Prohibited Uses	30
23.1 Generally allowed low-risk support	30

23.2 Uses requiring review	31
23.3 Prohibited uses	31
24. Public Communications and Synthetic Media	31
25. Data Protection, Security, and Records	32
26. AI Review Process	32
27. Procurement and Vendor Requirements	32
28. AI Inventory, Training, and Monitoring	33
29. AI Incident Response	33
Digital Accessibility and Online Documents	35
30. Policy Statement and Legal Standard	35
31. Web-First Rule	35
32. When a Fixed-Format Document May Be Used	35
33. Accessible Document Requirements	36
34. Priority Inventory and Remediation	36
35. Limited Federal Exceptions	36
36. Department Responsibilities and Issue Response	37
37. Public-Facing Web Accessibility Statement	37
37.1 Our commitment	37
37.2 Website accessibility features	37
37.3 Third-party content	38
37.4 Assistance and barrier reporting	38
Privacy and Personal Information	40
38. Citywide Privacy Commitment and Scope	40
39. Information the City May Collect	40
40. How the City Uses Information	40
41. Information Sharing and No-Sale Rule	40
42. Photographs, Video, and Promotional Use	41

43. Children's Privacy	41
44. Data Security, Retention, and Incident Response	41
45. Access, Correction, Removal, and Deletion Requests	42
46. Third-Party Services, Policy Changes, and Accountability	42
47. Parks and Recreation Application Privacy Addendum	42
47.1 Application information and use	42
47.2 Sharing, advertising, and security	43
47.3 User choices, children, and outside links	43
Film Coordination and Permit Intake	45
48. Purpose and Administrative Status	45
49. When City Coordination Is Required	45
50. Lead Office and Submission Timing	45
51. Application Requirements	45
52. Impact Classification	46
53. Review and Decision Process	46
54. Insurance, Deposits, Fees, and City Services	46
55. Public Safety, Neighborhoods, and Accessibility	47
56. Filming City Employees and Facilities	47
57. Compliance, Revocation, and Records	47
AI Use-Case Intake Checklist	48
AI Output Release Checklist	49
Accessible Publishing Checklist	50
Film Application Review Checklist	51
Privacy Request and Review Checklist	52
Authorities and Reference Standards	53

PART I

Department Foundations

Authority, responsibility, standards, and workflow for one clear City voice.

1. Purpose and Unified Standard

The City of Anniston communicates as one public institution. This manual establishes a unified standard for accurate, timely, accessible, secure, lawful, and trustworthy public communication across departments and platforms.

The Public Relations Department is the City's central communications authority. Departments remain responsible for the accuracy of their subject-matter information, while Public Relations is responsible for Citywide voice, publishing standards, public presentation, channel coordination, and communications risk management.

Public trust standard

Every communication issued in the City's name must be able to withstand public, legal, accessibility, records, and factual review. Speed never excuses inaccuracy, fabrication, exclusion, or avoidable risk.

2. Scope and Order of Authority

This manual applies to official City communications and to City business conducted through any account, device, platform, vendor, production, or document format. It supplements applicable ordinances, personnel rules, records schedules, procurement requirements, cybersecurity standards, emergency procedures, and law.

- If this manual conflicts with federal or state law, an adopted ordinance, a controlling court order, or an approved emergency command structure, the controlling authority governs.
- A department procedure may add operational detail but may not reduce the requirements in this manual or create a conflicting City communication standard.
- Questions involving legal exposure, public records, personnel, privacy, accessibility, safety, procurement, or enforcement must be referred to the responsible City office before release or implementation.

3 Communications Governance

Role	Core responsibility
City Manager	Directs municipal administration; approves major, sensitive, emergency, or policy-significant communications.
Public Relations Director	Sets communication strategy and standards; assigns work; reviews high-impact content; serves as primary media liaison unless otherwise directed.
Public Relations Staff	Create, schedule, publish, monitor, archive, and report on approved content; maintain brand and accessibility standards.
Department Heads	Provide timely, complete, and accurate source information; approve operational facts; identify subject-matter contacts.
Administrative Assistants / Designees	Submit requests through the approved process and coordinate drafts, deadlines, and approvals for their departments.
City Council	Establishes policy through collective official action. Individual members do not direct staff or speak for the City unless authorized.

3.1 Department Administration and Standard Operating Procedures

The Public Relations Department operates within General Government under the City Manager. In the council-manager form, the City Council sets policy through official action, the City Manager directs administration and staff, and Public Relations communicates City business accurately, promptly, accessibly, and without political advocacy.

The Public Relations Director coordinates with department heads, designated administrative assistants, and subject-matter staff to identify needs, verify source information, select channels, and produce, publish, and preserve public notices, news releases, web and social content, graphics, photography, video, media responses, and event coverage. The originating department approves facts and operations; Public Relations controls Citywide voice, branding, accessibility, production quality, scheduling, and publishing readiness.

Routine work follows the approved workflow. Emergencies and matters involving personnel, litigation, law enforcement, elections, financial commitments, contested facts, legal rights, or significant City policy are elevated to the City Manager and responsible offices. Requests are prioritized by public safety, legal or operational urgency, citywide impact, deadline, and available resources. Requests from individual officials follow the same process and may not present a personal, political, or campaign position as the City's official position.

4 Department Request and Approval Workflow

All communication requests should use the approved departmental process. The originating department supplies and approves operational facts; Public Relations prepares the communication for public release.

- 1 Submit**
Send the purpose, audience, key facts, requested channels, deadline, source materials, and departmental contact.
- 2 Review and prioritize**
Public Relations confirms scope, urgency, required approvals, accessibility needs, and production schedule.
- 3 Develop**
Public Relations drafts, designs, edits, or produces the content and coordinates needed subject-matter review.
- 4 Approve and publish**
The originating department approves facts and operations. Public Relations completes the final communication and publishes it through approved channels.
- 5 Preserve and evaluate**
Public Relations retains the final material and, when useful, reviews reach, engagement, media response, or lessons learned.

5 Temporary Modified Duty

The department may support temporary modified duty when an injury, illness, or medical condition limits fieldwork. Human Resources approval is required, and assignments must match the employee's restrictions, available work, and operational needs.

Assignments may include scheduling, writing and editing, graphic design, video editing, website management, media coordination, analytics, records management, and other office-based work. When feasible, another team member may cover ribbon-cuttings, radio appearances, field videography, and public events.

Each assignment is individualized and reviewed as restrictions, available work, or departmental needs change. Modified duty is temporary and does not replace rights or procedures under City personnel rules, leave policies, workers' compensation, or disability-accommodation law.

Core safeguards

Individual review | HR approval | Productive work within restrictions | Periodic reassessment

PART II

Social Media Policy

Official accounts, employee responsibilities, public engagement, records, accessibility, security, and emergency communication.

1. Purpose and Policy Statement

The City of Anniston uses social media to provide timely, accurate, accessible, and useful information about City services, decisions, programs, facilities, emergencies, events, and opportunities for public participation. This policy establishes one Citywide standard for creating, managing, securing, archiving, and moderating official social media accounts.

Official social media is an extension of City government. Content must support a legitimate municipal purpose, protect public trust, comply with applicable law, and reflect the same professionalism expected in any other official communication. Speed is valuable, but accuracy, fairness, accessibility, security, and legal compliance control.

Core rule

The City will never remove, hide, suppress, or restrict a person's comment solely because the comment criticizes the City, its policies, its employees, or its officials, or because the City disagrees with the person's viewpoint.

2. Scope

This policy applies to:

- Every social media account, page, profile, channel, group, livestream, story, advertising account, or similar platform created, owned, controlled, funded, or operated by the City or on the City's behalf.
- All City departments, offices, boards, commissions, facilities, programs, and affiliated pages that use the City name, seal, branding, staff time, equipment, email, funds, or other resources.
- Employees, officials, volunteers, interns, contractors, vendors, and other authorized users when they create, approve, publish, moderate, archive, or otherwise manage City social media.
- Official business conducted through a personal or unofficial account, regardless of who owns the device or account.

This policy does not convert a genuinely personal account into a City account merely because its owner is employed by or elected to the City. Section 14 addresses the line between personal and official use. Separate public safety, evidentiary, investigative, or emergency communications procedures remain in effect where they are more specific and consistent with this policy.

3. Definitions

Authorized user	A person approved in writing to access or manage a City social media account.
City social media account	Any account the City creates, owns, controls, funds, staffs, or presents as an official source of City information.
Comment	Any reply, reaction, mention, tag, review, image, video, link, direct message, or other user-generated submission made through a social media platform.
Limited public forum	An interactive space the City opens for public comment on defined subjects and regulates through reasonable, viewpoint-neutral rules.
Official business	Communication, action, or information connected to the powers, duties, services, decisions, operations, or interests of the City.
Personal account	An account created and maintained by an individual in a private capacity, without City ownership or control, and not used to exercise actual governmental authority.
Record	Recorded information made or received in connection with City business, regardless of medium, location, ownership of the device, or whether it remains visible on a platform.
Social Media Administrator	The Public Relations Director or another Communications Department designee responsible for Citywide account governance under this policy.

4. Governance and Responsibility

Role	Primary responsibility
City Manager	Executive oversight; approval of high-risk communications; designation of emergency authority; final administrative enforcement.
Communications Department / Public Relations Director	Citywide standards, account inventory, content coordination, administrator training, brand management, moderation oversight, analytics, and annual policy review.
Department heads	Accuracy and operational approval of departmental information; selection and supervision of authorized users; prompt notice of staffing and access changes.
Information Technology	Account security standards, approved devices and applications, incident response, access recovery, and technical support.
City Clerk / records custodian	Records classification, retention, legal holds, preservation, destruction notices, and public records request coordination.
Human Resources	Employee training and discipline; consistency with personnel rules, protected employee rights, and due process.
City Attorney	Legal review of moderation, blocking, litigation holds, high-risk content, First Amendment issues, privacy, and interpretation.
Authorized users	Compliance with this policy; accurate, accessible, secure, and properly approved publishing; preservation and escalation of issues.

The Communications Department may issue platform-specific procedures, templates, accessibility checklists, approval workflows, and administrator instructions consistent with this policy. Departmental rules may be more restrictive when operationally necessary, but may not authorize viewpoint discrimination or reduce recordkeeping, accessibility, or security requirements.

5. Account Approval, Ownership, and Closure

5.1 Approval before creation

No City account may be created without written approval from the department head and the Social Media Administrator. The request must identify the municipal purpose, intended audience, platform, content plan, staffing, moderation plan, accessibility plan, records method, and business need that cannot be met through an existing account.

5.2 City ownership and account inventory

- Accounts must use a City-controlled email address and recovery method. A personal email address or phone number may not be the sole owner, login, or recovery method.
- The Communications Department will maintain a current inventory of each account's platform, URL, purpose, department, primary and backup administrators, creation date, recovery method, archive method, and status.
- Usernames, page names, logos, bios, and contact information must clearly identify the account as official and link to AnnistonAL.gov when the platform permits.
- Account credentials, content, contacts, followers, messages, analytics, advertising assets, and related data are City property to the extent permitted by law and platform terms.
- Authorized users may not sell, transfer, rename, merge, deactivate, or delete a City account without written approval from the Social Media Administrator, Information Technology, records custodian, and department head.

5.3 Inactive or closing accounts

Before an account is closed, the City must preserve required records, redirect the audience to an active official source, revoke access, remove connected third-party applications, document the closure, and retain proof of the action. Dormant accounts will be reviewed at least annually and closed when they no longer serve a documented municipal purpose.

6. Access Control and Cybersecurity

- Use multifactor authentication on every platform that supports it. Phishing-resistant authentication is preferred when available.
- Use unique, strong credentials stored only in a City-approved password manager. Credentials may not be sent through ordinary email, text messages, or personal messaging applications.
- Apply least-privilege access. Each administrator must use an individually attributable login where the platform allows; generic shared administrator profiles are disfavored.
- Maintain at least two current City-controlled administrators for continuity, while limiting access to the smallest practical number of people.
- Review account access at least quarterly and immediately after a transfer, separation, contractor change, suspected compromise, or change in duties. Remove unnecessary access the same business day the change takes effect.

- Use City-approved devices, networks, scheduling tools, link shorteners, analytics, integrations, and advertising platforms. Third-party applications require Information Technology approval before connection.
- Do not approve unexpected login prompts, disclose verification codes, or respond to credential requests. Suspected phishing, impersonation, takeover, or unauthorized access must be reported immediately.

Security incident

An authorized user who suspects compromise must stop nonessential posting, preserve evidence, contact Information Technology and the Social Media Administrator immediately, revoke or rotate access as directed, and avoid public speculation. Any public notice will be coordinated with the City Manager and City Attorney.

7. Content Standards and Approval

7.1 Municipal purpose and voice

Official content must advance a legitimate City purpose and be factual, timely, service-oriented, and understandable to the intended audience. The City may communicate with warmth and personality, but official posts must remain professional and consistent with the City's role as a public institution. Accounts may not be used for personal disputes, retaliation, ridicule, private business promotion, or content designed primarily to benefit an employee, official, candidate, political party, or outside organization.

7.2 Accuracy, sourcing, and corrections

- Confirm names, dates, times, addresses, links, amounts, quotations, statistics, legal status, and responsible department before publication.
- Use primary City records or authoritative external sources. Attribute third-party facts, images, and quotations when appropriate.
- Do not announce a policy, contract, personnel action, investigation result, emergency condition, or official decision before the responsible authority has approved release.
- Correct material errors promptly. When an edit could mislead readers about what was originally published, add a visible correction note or publish a follow-up instead of silently changing or deleting the post.
- Preserve the original and corrected versions when required by the records schedule or a legal hold.

7.3 Approval matrix

Content type	Minimum approval
Routine service information	Authorized user under the department's approved content workflow.
Citywide announcement or policy explanation	Communications Department and responsible department; City Manager review when material.
Personnel, litigation, investigations, death or serious injury, public health, security-sensitive information, or highly contested matters	Communications Department plus City Manager and City Attorney or other responsible authority, as applicable.
Emergency warning or active incident	Designated Public Information Officer or Incident Command under the emergency communications procedure.
Paid or boosted content	Communications Department plus applicable purchasing, finance, and platform authorization.

7.4 Privacy, dignity, copyright, and releases

- Do not publish confidential, privileged, sealed, security-sensitive, medical, personnel, juvenile, victim, financial, authentication, or other legally protected information.
- Follow the City's Privacy Policy and approved release procedures for photographs, video, testimonials, and program information.
- Obtain appropriate parent or guardian permission before identifying or featuring a minor in a planned promotional post, unless the City Attorney has approved a different lawful practice for incidental public-event coverage.
- Avoid pairing a minor's full name with school, schedule, home address, routine location, or other information that could create a safety risk. Do not tag a minor's personal account without documented permission.
- Use only content the City created, licensed, received permission to use, or may lawfully use. A web search result is not permission.
- Treat people with dignity, especially during emergencies, enforcement actions, medical events, homelessness, grief, or other vulnerable circumstances.

7.5 Links, likes, shares, follows, and endorsements

A link, share, like, reaction, follow, tag, or repost should serve a City purpose and does not necessarily constitute endorsement. Accounts should avoid selective interactions that create the appearance of political favoritism, commercial endorsement, or unequal treatment. Contests, giveaways, sponsorships, and co-branded campaigns require advance approval and compliance with applicable procurement, ethics, platform, and records rules.

8. Accessibility and Inclusive Communication

The City uses WCAG 2.1 Level AA as the operational standard for digital content it provides or makes available, including content distributed through third-party platforms. Accessibility is part of the publishing process, not an optional correction after a complaint.

- Provide meaningful alternative text for informative images. Mark decorative images as decorative when the platform supports it.
- Provide accurate captions for prerecorded video with speech and review automated captions before publication. Provide transcripts or equivalent text for material audio content.
- For livestreams, enable available live-captioning tools and post a corrected captioned recording or transcript as soon as practicable when the information remains relevant.
- Do not place essential information only inside a graphic, flyer, screenshot, video, or audio clip. Repeat dates, times, locations, deadlines, links, and action steps in accessible post text or on an accessible City webpage.
- Use sufficient color contrast, legible type, plain language, descriptive link text, logical reading order, and CamelCase for multiword hashtags. Use emojis sparingly and do not use emoji strings as a substitute for words.
- Avoid flashing content and do not rely on color, sound, shape, or location alone to communicate meaning.
- Publish accessible documents whenever possible. If a platform or document cannot provide equal access, provide an effective alternative method and a clear contact for assistance.
- Respond promptly to accessibility problems and coordinate recurring issues with the City's ADA Coordinator and Communications Department.

Practical standard

If a resident cannot understand or act on a post without seeing the graphic, hearing the audio, or distinguishing a color, the post is not finished.

9. Artificial Intelligence, Automation, and Synthetic Media

- City social media may not use AI-generated or materially AI-altered images, video, audio, voices, or likenesses as representations of real City people, places, events, projects, or conditions.
- Generative AI may be used only as an authorized composition or brainstorming aid for text. A City employee remains responsible for the final work and must independently verify every fact, quotation, date, link, legal assertion, and attribution before approval.
- Confidential, privileged, personally identifiable, security-sensitive, procurement-sensitive, personnel, health, investigative, or nonpublic information may not be entered into a public or unapproved AI service.
- AI output may not be used to fabricate quotations, public comments, endorsements, evidence, incidents, public sentiment, meeting content, or interactions that did not occur.
- Automated captions, translations, summaries, and transcripts must be reviewed by a person when they carry material meaning. Machine translation should be labeled when accuracy cannot be verified.
- Scheduled posts and automated replies require advance approval, clear ownership, and monitoring. Fully autonomous public posting is prohibited unless specifically authorized in writing by the City Manager after Communications, Information Technology, and legal review.
- Ordinary editing tools such as cropping, exposure correction, noise reduction, resizing, and compression may be used so long as they do not materially misrepresent the subject.

Nothing in this section prevents the City from publishing educational material about AI, displaying clearly labeled AI content when necessary to explain or warn about it, or using an approved automated public-service tool governed by a separate policy.

10. Public Comments and Moderation

10.1 Forum designation and notice

City social media accounts exist principally to distribute City information. When the City enables and accepts public comments, the interactive portion of the account is a limited public forum for comments reasonably related to the subject of the City's post. The public-facing guidelines in Appendix A must be linked, pinned, or otherwise made reasonably available before routine moderation begins.

10.2 Viewpoint-neutral rule

Protected criticism
Disagreement, criticism, allegations of poor performance, harsh tone, political viewpoint, or offensive or profane language standing alone are not sufficient grounds for removal. The City should generally answer false or misleading claims with accurate information rather than remove them.

10.3 Content eligible for restriction

A comment may be hidden, removed, reported, or otherwise restricted only when the action is authorized below, is applied consistently without regard to viewpoint, and is documented. The narrowest effective action should be used. Eligible categories are:

- 1 Comments that are not reasonably related to the subject of the City's post, interpreted broadly in favor of allowing discussion. On a post that invites general feedback, this category does not apply.
- 2 Spam, scams, phishing, malicious code, deceptive links, automated flooding, substantially identical repetitive posts, or commercial solicitations unrelated to City business.
- 3 Content that satisfies an applicable legal definition of a true threat, incitement to imminent lawless action, obscenity, unlawful harassment, or solicitation of a specific criminal act. Mere insult, advocacy, hyperbole, or unpopular opinion does not qualify.
- 4 Personal identifiers or sensitive information that creates a material privacy or safety risk, including Social Security numbers, financial account data, authentication credentials, protected medical information, private contact details, or doxing.
- 5 Content that unlawfully infringes copyright, trademark, or another intellectual property right, after sufficient verification.
- 6 Impersonation of the City, a City department, an employee, or an official; a false claim of authority to speak for the City; or manipulated account information reasonably likely to deceive the public about an official source.
- 7 Information whose publication is prohibited by law, court order, or binding confidentiality requirement, or narrowly identified operational details that create a specific and imminent safety or cybersecurity risk, after legal or emergency review when practicable.
- 8 Content that materially interferes with the technical operation of the page or another person's ability to participate, such as high-volume flooding, provided ordinary repeated criticism is not treated as disruption.

10.4 Moderation procedure

- 1 Before taking action, capture the comment, username, date and time, URL or post, surrounding context, and any available metadata. For an immediate threat or malicious link, secure the account first and document as soon as practicable.

- 2 Identify the exact rule and apply it without regard to the user's identity, affiliation, history of criticism, or viewpoint. When uncertain, leave the comment visible and escalate to the Social Media Administrator.
- 3 Use the narrowest action. Hiding a qualifying comment is generally preferred to deletion when the platform allows it and the preserved record remains available to the City.
- 4 Enter the action in the moderation log, including the reviewer, reason, evidence preserved, action taken, notice provided, and final disposition.
- 5 Notify the user when practical, state the specific rule, and provide the appeal method. No notice is required before addressing malware, account compromise, automated spam, or a credible emergency threat.
- 6 Refer credible threats, suspected crimes, child-safety concerns, or emergency information to the appropriate public safety authority. Moderation is not a substitute for response or investigation.

10.5 Blocking, muting, and comment closure

Because platform-wide blocking can prevent access to multiple official discussions, an authorized user may not block or broadly restrict a person without written approval from the Social Media Administrator and City Attorney. Blocking should be limited to automated accounts, demonstrated security threats, or repeated policy violations after notice when a narrower tool is unavailable or ineffective. Any restriction must be time-limited unless continued restriction is legally approved, documented, and reviewed at least every 30 days.

The City may disable comments for an account or a defined class of posts for a documented operational reason, provided the decision is made and applied without regard to viewpoint. Comments may not be closed merely because criticism appeared. Post-specific closure after discussion begins requires Communications and legal review except during an immediate technical or safety incident.

10.6 Appeals

A person may request review of a moderation decision by contacting the Communications Department through the current contact information at AnnistonAL.gov/communications within 30 calendar days. The appeal should identify the account, post, approximate date, username, and disputed action. A person not involved in the original decision should review the action when practicable, consult the City Attorney when needed, and provide a written response within 10 business days or notice that additional time is required. If the action was inconsistent with this policy, the City will restore the content or access when technically possible and correct the moderation log.

11. Records, Retention, and Public Records Requests

Social media records are governed by their content and function, not by the platform or device on which they appear. City posts, comments, edits, direct messages, deleted or hidden material, approvals, advertisements, analytics, moderation decisions, and account records may be public records and must be managed under Alabama law and the applicable Records Disposition Authority (RDA).

- Preserve a complete copy or snapshot of each City website and social media site at least annually and whenever significant changes are made. Under the Alabama Municipalities RDA, these snapshots are permanent records.
- Classify and retain individual posts, messages, comments, replies, and attachments according to the applicable record series. For example, routine correspondence is generally retained for three years under the current Municipalities RDA, while records connected to policy, litigation, personnel, procurement, emergencies, grants, law enforcement, or another function may have a different or permanent retention.
- Do not rely on a platform to preserve City records. Platform deletion, account suspension, disappearing-message features, or loss of vendor access does not remove the City's preservation duty.

- Capture removed or hidden comments and the associated moderation record before action whenever practicable.
- Do not delete or alter records subject to a public records request, audit, investigation, subpoena, claim, anticipated litigation, or legal hold, even if the ordinary retention period has expired.
- Destroy records only through the City-approved records process and only after all RDA, audit, destruction-notice, and legal-hold requirements are satisfied.
- Forward any social media request that reasonably appears to seek City records to the City Clerk or records custodian promptly. Do not promise disclosure, denial, cost, or completion time from the social media account.

Official channel

A comment or direct message is not the City's designated process for a public records request, legal notice, claim, appeal, application, bid, service of process, or other formal filing. Staff should direct the sender to the appropriate City office and preserve the communication as required.

12. Direct Messages, Service Requests, and Customer Care

- State clearly that social media accounts are not monitored continuously and are not emergency channels. Direct emergencies to 911.
- Use approved scripts to acknowledge messages and direct residents to the correct department, service request portal, Customer Service line, City Clerk, or public safety contact.
- Do not request or encourage a person to post sensitive information publicly. Move the interaction to an approved secure channel when personal information is needed.
- Do not provide individualized legal, medical, tax, licensing, benefits, employment, enforcement, or eligibility determinations through social media unless an approved process specifically authorizes it.
- If a message reports a hazard, threat, abuse, neglect, crime, infrastructure failure, or urgent service problem, preserve it and escalate it promptly under the responsible department's procedure.
- A response on social media does not replace an official work order, report, complaint, application, or case record unless the City's approved system expressly integrates the interaction.

13. Emergency and Crisis Communications

During an emergency, the designated Public Information Officer or Incident Command structure controls incident communications. Departments must coordinate facts, timing, terminology, protective actions, maps, closures, and corrections with the lead authority and partner agencies. Official warnings should identify the source, affected area, time, action residents should take, and where updates will appear.

- Prioritize life safety, actionable instructions, accessibility, and verified facts over branding or engagement.
- Time-stamp rapidly changing information and update or replace stale instructions clearly.
- Do not identify victims, juveniles, medical conditions, tactical positions, responder vulnerabilities, or investigative details unless release is authorized.
- Monitor rumors and questions. Correct consequential misinformation with a clear source and avoid amplifying low-impact rumors unnecessarily.

- Coordinate account access, backups, power, connectivity, and alternate publishing routes before an incident occurs.
- After the incident, preserve the record, document material corrections, and conduct an after-action review when warranted.

14. Employees, Officials, and Personal Accounts

14.1 Personal expression

City employees and officials retain rights to speak as private citizens, subject to applicable law and City personnel, ethics, confidentiality, and workplace rules. This policy is not intended to restrict protected speech, lawful political activity, reporting of wrongdoing, participation in public affairs, or other legally protected conduct. Any employment action involving personal social media must be reviewed by Human Resources and, when appropriate, the City Attorney.

14.2 Keeping personal and official activity distinct

- A personal account should be clearly labeled as personal. A disclaimer such as 'views are my own' may reduce confusion but does not control if the account is actually used to exercise City authority.
- Do not use City logos, account names, staff, equipment, email, funds, exclusive announcements, or official access in a way that makes a personal account appear to be an official City source.
- Do not disclose nonpublic City information or conduct official business through disappearing messages or an account the City cannot preserve.
- If official business is received or conducted on a personal account, promptly preserve and forward the record to the appropriate City system or custodian. Do not delete it to avoid disclosure or retention.
- Employees may identify their employment, but may not claim to speak for the City unless authorized. Media inquiries concerning City business should be referred through the approved communications process.
- Personal use of social media during work time or on City equipment must comply with personnel and technology rules and must not interfere with duties, service, security, or operations.

14.3 Elected and appointed officials

Officials who maintain both personal and official accounts should keep them clearly separate. Under *Lindke v. Freed*, social media conduct may be attributable to government when an official possesses actual authority to speak for government on a matter and purports to exercise that authority in the relevant posts. Account labels, content, function, use of staff or public resources, exclusive announcements, and moderation practices may all matter. Officials should obtain legal advice before blocking users or mixing official business with a personal account.

15. Elections, Campaigns, and Political Activity

- City accounts, staff time, equipment, advertising funds, email lists, logos, and other City resources may not be used to endorse or oppose a candidate, political party, ballot committee, or campaign; solicit campaign support or contributions; or coordinate campaign communications.
- The City may publish neutral, service-oriented election information within its lawful responsibilities, including registration information, qualifying notices, deadlines, polling information, accessibility, office closures, and certified results.

- Coverage of an incumbent official must have a bona fide municipal purpose and follow ordinary communications standards. Content should not be timed, framed, targeted, or promoted primarily to influence an election.
- Candidate or campaign comments are governed by the same viewpoint-neutral public comment rules as all other comments. Political advocacy is not removable merely because it is political; it may be restricted only under an otherwise applicable rule, such as being off-topic to a narrowly defined post.
- Employees and officials engaging in lawful personal political activity must do so in a private capacity and must not imply City sponsorship or use City resources.

16. Training, Monitoring, and Enforcement

- Before receiving access, each authorized user must complete training on this policy, platform security, records, accessibility, privacy, public comments, emergency escalation, and applicable department procedures, and must sign the acknowledgment in Appendix C.
- Refresher training is required at least annually and after a material policy, legal, platform, or security change.
- The Communications Department will review the account inventory, administrator access, public-facing guidelines, moderation logs, archive status, and inactive accounts at least annually. Information Technology may require more frequent security reviews.
- Unauthorized accounts or uses may be suspended, transferred, renamed, or closed after preservation and review. Violations may result in removal of access, corrective training, or discipline consistent with law, City personnel rules, contracts, and due process.
- No person may retaliate against another person for criticizing the City, requesting records, appealing moderation, reporting a concern, or exercising a protected right.

17. Administration, Exceptions, and Review

Questions about this policy should be directed to the Communications Department. The City Manager may approve a written operational exception after consultation with the Social Media Administrator, Information Technology, records custodian, Human Resources, or City Attorney, as relevant. No exception may authorize unlawful discrimination, viewpoint-based moderation, destruction of records, disclosure of protected information, or a reduction of legally required accessibility or security.

If a provision conflicts with controlling law, a court order, an approved emergency procedure, or a more specific mandatory rule, the controlling authority governs and the remainder of this policy continues in effect. The Communications Department will coordinate review at least annually and recommend updates when law, technology, City operations, or platform features materially change.

Appendix A

Public-Facing Social Media Comment Guidelines

Ready to publish

This appendix is written for the public and may be linked or adapted for an account's About section. Platform character limits may require a short version that links to the complete text on AnnistonAL.gov.

Welcome

The City of Anniston uses social media to share information about City services, programs, decisions, emergencies, events, and opportunities to participate. We welcome comments that are reasonably related to the subject of the City's post.

Public forum and viewpoint neutrality

When comments are enabled, the interactive portion of this account is a limited public forum for discussion related to the subject of the City's post. The City applies these rules without regard to viewpoint. Criticism of the City, its employees, officials, services, or policies will not be removed merely because it is critical, harsh, unpopular, or disagrees with the City.

Comments that may be restricted

The City may hide, remove, report, or otherwise restrict a comment that falls within one or more of these categories:

- Not reasonably related to the subject of the City's post, unless the post invites general feedback.
- Spam, scams, phishing, malicious links or code, automated flooding, substantially identical repetitive posts, or unrelated commercial solicitations.
- A legally recognized true threat, incitement to imminent lawless action, obscenity, unlawful harassment, or solicitation of a specific criminal act.
- Sensitive personal information that creates a material privacy or safety risk, such as Social Security numbers, financial account data, login credentials, protected medical information, private contact details, or doxing.
- Content that unlawfully infringes copyright, trademark, or another intellectual property right.
- Impersonation of the City or a false claim of authority to speak for the City.
- Information prohibited from publication by law, court order, or a binding confidentiality requirement, or narrowly identified details creating a specific and imminent safety or cybersecurity risk.
- Content that materially disrupts the technical operation of the page or another person's ability to participate through high-volume flooding or similar conduct.

Blocking and appeals

The City uses the narrowest practical moderation tool and does not block users merely for criticism or disagreement. If you believe your comment or access was restricted incorrectly, you may request review within 30 calendar days by contacting the Communications Department using the current contact information at AnnistonAL.gov/communications. Please identify the account, post, approximate date, username, and disputed action.

Records and privacy

Comments, usernames, profile information, and direct messages may be visible to the public, retained as public records, and disclosed as required by law. Do not post sensitive personal information. The City does not control a platform's collection, use, or disclosure of information; review the platform's privacy terms before participating.

Not an emergency or formal filing channel

This account is not monitored continuously. Call 911 for emergencies. A social media comment or message is not the City's designated method for a public records request, legal notice, claim, appeal, application, bid, service request, service of process, or other formal filing. Visit AnnistonAL.gov or contact the appropriate City office.

Third-party content

A public comment, external link, share, reaction, or follow does not necessarily reflect the views of or constitute an endorsement by the City. The City may change these guidelines when required by law, operations, security, accessibility, or platform changes and will post the current version on AnnistonAL.gov.

Suggested short account notice

Short notice

Official City of Anniston account. Comments are subject to viewpoint-neutral guidelines. Criticism is allowed; off-topic content, spam, true threats, sensitive personal information, impersonation, unlawful content, and technical disruption may be restricted. Not monitored 24/7. Call 911 for emergencies. Full policy and appeals: AnnistonAL.gov.

Appendix B

Administrator Checklists and Moderation Record

B.1 Before publishing

- Municipal purpose is clear; responsible department has approved the facts.
- Names, dates, times, address, amount, quotation, link, and call to action are verified.
- The approval level in Section 7.3 has been satisfied.
- No confidential, privileged, restricted, or unnecessary personal information is included.
- Image, video, music, font, logo, and quotation rights or permissions are documented.
- Minor and participant releases are complete when required.
- Alt text, captions, transcript, contrast, plain language, link text, and graphic text have been checked.
- Any AI-assisted text has been independently verified and edited; no prohibited synthetic media is used.
- Record capture and archive method is active.

B.2 Before moderating

- Would the same action be taken if the viewpoint were reversed?
- Is the comment within a specific category in Section 10.3?
- Is the comment merely critical, harsh, offensive, political, or alleged to be false? If so, leave it unless another category applies.
- Has the surrounding conversation and original City post been reviewed?
- Has evidence been captured before action?
- Is a narrower tool available?
- Does the action need escalation to Communications, Legal, Information Technology, or Public Safety?

B.3 Moderation record fields

Field	Entry
Account / platform	
City post URL and subject	
Commenter username / profile URL	
Comment date and time	
Evidence file or archive location	
Exact policy category	
Action taken and time	
Moderator name	
Notice sent / method	
Escalation and reviewer	
Appeal received / outcome	
Record series / retention / hold	

For a true threat, emergency, suspected crime, child-safety issue, or malicious link, preserve what is safely available and contact the appropriate authority immediately. Do not delay response merely to complete the form.

Appendix C

Authorized User Acknowledgment

I acknowledge that I have received, read, and understand the City of Anniston Social Media Policy and the platform-specific procedures applicable to my role. I understand that access is limited to authorized City business and may be removed at any time. I agree to protect credentials, use approved tools, follow content and approval standards, create accessible communications, preserve records, apply comment rules without regard to viewpoint, report incidents promptly, and return or transfer all City account access when directed.

Authorized user name	
Department / title	
Accounts / platforms authorized	
Signature	
Date	
Supervisor approval	
Communications approval	

Appendix D

Legal and Administrative References

Reference note

These authorities support the policy and are provided for administrators and legal counsel. They do not replace legal advice. The City Attorney should confirm material changes in governing law and local procedure during policy review.

1. U.S. Constitution, First Amendment
<https://constitution.congress.gov/constitution/amendment-1/>
2. 42 U.S.C. Section 1983
<https://uscode.house.gov/view.xhtml?req=granuleid:USC-prelim-title42-section1983>
3. Lindke v. Freed, 601 U.S. 187 (2024)
https://www.supremecourt.gov/opinions/23pdf/22-611_ap6c.pdf
4. Code of Alabama 1975, Section 36-12-40 et seq. - Public Records
<https://alison.legislature.state.al.us/code-of-alabama?section=36-12-40>
5. Code of Alabama 1975, Sections 41-13-22 through 41-13-24 - Local records
<https://alison.legislature.state.al.us/code-of-alabama?section=41-13-23>
6. Alabama Department of Archives and History - Municipalities Records Disposition Authority, including Section 18.18
<https://archives.alabama.gov/RDA?id=21>
7. Alabama Department of Archives and History - Local agency records guidance
<https://archives.alabama.gov/manage/local/>
8. U.S. Department of Justice - Title II web and mobile accessibility rule fact sheet
<https://www.ada.gov/resources/2024-03-08-web-rule/>
9. U.S. Department of Justice - 2026 interim final rule extending compliance dates
<https://www.ada.gov/assets/pdfs/2026-ifr.pdf>
10. Web Content Accessibility Guidelines (WCAG) 2.1
<https://www.w3.org/TR/WCAG21/>
11. Cybersecurity and Infrastructure Security Agency - Multifactor authentication
<https://www.cisa.gov/MFA>
12. City of Anniston - Web Accessibility Statement
<https://anniston.al.gov/web-accessibility/>
13. City of Anniston - Privacy Policy
<https://anniston.al.gov/wp-content/uploads/2024/12/Privacy-Policy-City-of-Anniston-Alabama.pdf>
14. City of Anniston - Communications Department
<https://anniston.al.gov/communications/>
15. City of Anniston - City Clerk
<https://anniston.al.gov/city-clerk/>

The Alabama Municipalities RDA classifies annual or significant-change snapshots of municipal websites and social media sites as permanent records and lists routine correspondence as a temporary record generally retained for three years. The applicable record series must always be determined from content and function, and legal holds override ordinary destruction schedules.

The U.S. Department of Justice's current Title II rule adopts WCAG 2.1 Level AA for covered state and local government web content and mobile apps. The 2026 interim final rule extends the compliance date for public entities with populations below 50,000, and for special district governments, to April 26, 2028. Existing Title II duties to provide effective communication and equal access remain in effect before that date.

PART III

Artificial Intelligence Policy and Governance

A risk-based system for responsible use, procurement, review, transparency, and human accountability.

18. Purpose, Scope, and Core Rule

This part governs the selection, procurement, testing, use, monitoring, and retirement of artificial intelligence systems used for City business. It applies to stand-alone AI tools, AI features embedded in existing software, automation that produces recommendations or decisions, generative AI, synthetic media, meeting tools, chatbots, predictive systems, and vendor services that use AI on the City's behalf.

Core rule

AI may support City work, but it may not replace accountable human judgment. Every City employee remains responsible for the facts, decisions, records, rights, security, accessibility, and public consequences of work produced with AI.

19. Definitions

Term	Meaning
AI system	Technology that uses data or models to generate content, predictions, recommendations, classifications, insights, or decisions that support or affect City activity.
Generative AI	AI that creates or transforms text, images, video, audio, software code, or other content in response to instructions or data.
Synthetic media	Media generated or materially altered by AI in a way that depicts or imitates a person, place, event, voice, action, or condition.
Business owner	The department accountable for the purpose, data, operation, outcomes, and continued need for an AI use case.
Human oversight	Meaningful review by a qualified person who can understand, challenge, correct, reject, stop, and document an AI-supported output or action.
Material change	A change in purpose, users, data, model, output, integration, vendor practice, performance, or risk that could alter the approved use.

20. Responsible AI Principles

- Lawful and purpose-limited: use AI only for a defined municipal purpose and within applicable authority.
- Human-led and accountable: identify the employee and department responsible for every use and outcome.
- Accurate and reliable: test outputs, verify facts, document limitations, and maintain a non-AI fallback for essential services.
- Private and secure: minimize data, use approved tools, protect credentials, and prohibit sensitive data in public AI services.
- Fair and rights-protective: assess bias, unequal impact, due process, opt-out, appeal, and accessibility before deployment.
- Transparent and explainable: provide notice and understandable explanations when AI materially affects the public or a City decision.

- Accessible and inclusive: require equal access for residents and employees with disabilities and avoid automating barriers.
- Proportionate: apply stronger review, testing, documentation, approval, and monitoring as potential harm increases.

21. Governance and Responsibility

The City Manager is the final administrative authority for AI use. The Public Relations Director coordinates governance for public communications and transparency. Information Technology coordinates technical security and approved-system controls. An AI Review Team will be assembled as needed from Public Relations, Information Technology, the City Attorney, Human Resources, Purchasing, Risk Management, the City Clerk or records officer, the business-owning department, and subject-matter experts.

- Departments must identify AI features before purchase, activation, pilot, integration, or material expansion.
- The business owner must name an accountable employee, define the public need, document alternatives considered, and maintain the approved controls.
- The City may pause, limit, or terminate any AI use that is inaccurate, unsafe, discriminatory, inaccessible, insecure, unauthorized, ineffective, or inconsistent with public trust.

22. Risk Classification

Level	Typical characteristics	Minimum treatment
Low	Optional, reversible, routine assistance; no sensitive data; no material effect on rights, services, safety, employment, or finances.	Supervisor approval; approved tool; human verification; no confidential data.
Moderate	Identifiable data, targeted service, public interaction, consequential recommendation, recurring external use, or limited impact on access or reputation.	Written threshold review; IT and business-owner controls; legal/PR review as relevant; testing, notice, monitoring, and inventory entry.
High	Rights- or safety-impacting; compulsory use; sensitive data; biometrics; public safety; employment; benefits; enforcement; critical infrastructure; automated or difficult-to-reverse decisions; realistic synthetic media.	Full impact assessment; City Attorney, IT, and City Manager approval; procurement safeguards; public engagement when appropriate; continuous oversight; documented appeal and shutdown process.

When risk is unclear
Classify the use at the higher level until the AI Review Team documents why a lower level is appropriate.

23. Allowed, Restricted, and Prohibited Uses

23.1 Generally allowed low-risk support

- Brainstorming, outlines, headlines, layout concepts, grammar, reading-level suggestions, and formatting assistance using non-sensitive information.

- Summarizing public or non-sensitive background material for internal working use, followed by review against the source.
- Routine software assistance such as spelling, autocomplete, transcription, or meeting notes when the tool, data handling, consent, and recordkeeping are approved.

23.2 Uses requiring review

- Public statements, press releases, policy explanations, official remarks, newsletters, website notices, translations, chatbots, or recurring public responses.
- AI-generated or AI-assisted graphics, illustrations, audio, video, voice, or likenesses for public use.
- Use involving law enforcement, emergencies, personnel, elections, finances, public benefits, permits, legal rights, public records, procurement, or sensitive services.
- New software purchases, vendor features, system integrations, pilots, or changes that introduce AI into a City process.

23.3 Prohibited uses

- Entering confidential, privileged, protected, personally identifiable, personnel, medical, financial, security-sensitive, procurement-sensitive, juvenile, victim, credential, or non-public incident information into an unapproved AI tool.
- Allowing AI to make a final decision that affects employment, discipline, benefits, enforcement, public safety, legal rights, access to City services, or another material interest without meaningful human authority and approved safeguards.
- Publishing fabricated facts, statistics, citations, quotations, public comments, meeting content, endorsements, evidence, incidents, sentiment, or interactions.
- Creating or altering media so the public could reasonably mistake a fictional event, statement, person, emergency, facility condition, or City action for an authentic one.
- Using AI to impersonate a resident, employee, official, candidate, organization, or member of the media; conduct unlawful surveillance; evade records duties; or conceal prohibited conduct.
- Using a consumer AI account, unapproved browser extension, personal subscription, or undisclosed vendor feature for City data or official automated action.

24. Public Communications and Synthetic Media

Official communications must remain human-led, fact-checked, accessible, and approved through the normal communications process. AI language may not be copied directly into publication without substantive human revision and source verification.

- Public Relations controls public-facing AI-assisted messaging and visual media.
- Every name, title, date, location, amount, quotation, statistic, citation, link, legal assertion, and factual claim must be checked against an authoritative source.
- AI-generated or materially altered images, video, audio, voices, or likenesses are not used to depict real City events, people, facilities, emergencies, or actions as authentic.
- A disclosure may be required when AI assistance is substantial and a reasonable person could misunderstand the origin or authenticity of the content.

- Automated translation, captioning, transcription, or summarization must be reviewed by a qualified person before it is treated as an official record or public statement.

25. Data Protection, Security, and Records

- Use only City-approved accounts, devices, integrations, and data environments. Multifactor authentication and least-privilege access are required where supported.
- Before use, determine what the vendor stores, where it is stored, who can access it, whether prompts or outputs train models, how long data is retained, and how data can be deleted or exported.
- Prompts, source files, outputs, approvals, testing, corrections, decisions, contracts, assessments, and incident records may be public records depending on content and function.
- Do not use AI to destroy, evade, obscure, or privately relocate a City record. Apply legal holds and retention schedules to AI-related records in coordination with the City Clerk.

26. AI Review Process

- 1 Proposal: The department describes the current process, public need, intended users, expected benefit, proposed data, vendor, cost, alternatives, accountable owner, and non-AI fallback.
- 2 Threshold analysis: The AI Review Team identifies whether AI is present and classifies the use as low, moderate, or high risk based on severity, reversibility, opt-out, data sensitivity, affected rights, and human control.
- 3 Assessment: Moderate- and high-risk uses complete an impact assessment. The vendor provides a fact sheet addressing data, models, testing, performance, bias, accessibility, security, storage, updates, limitations, monitoring, and correction.
- 4 Engagement: For high-risk or significant public-interest uses, the City seeks accessible community and stakeholder input, especially from people likely to be affected.
- 5 Decision: The responsible reviewing authorities approve, condition, return, deny, or escalate the use. Approval is limited to the documented purpose, data, users, vendor, and safeguards.
- 6 Pre-launch: Complete contracts, security controls, data rules, training, testing, inventory entry, public notice when appropriate, appeal channel, continuity plan, and shutdown procedure.
- 7 Monitoring: Measure accuracy, effectiveness, complaints, bias, accessibility, overrides, incidents, cost, and material changes. Re-review at least annually and before expansion or renewal.

27. Procurement and Vendor Requirements

Solicitations and contracts must require vendors to identify all AI components, including features added after purchase. Vendors must provide clear, non-technical answers sufficient for City review.

Review area	Required vendor information
System and purpose	What the system does, intended users and use cases, maturity, dependencies, and implementation plan.
Data	Training and testing data, City inputs, storage location, retention, sharing, deletion, ownership, and whether City data trains any model.

Review area	Required vendor information
Performance	Accuracy and effectiveness measures, test conditions, known limitations, failure modes, outliers, and conditions where performance degrades.
Fairness and accessibility	Bias testing, disparate-impact studies, representative data, assistive-technology compatibility, disability-user testing, and accessible feedback channels.
Human control	Explanations, review interfaces, override authority, audit logs, correction process, appeal support, and emergency shutdown.
Security and change	Security controls, incident notice, subcontractors, model updates, material-change notice, version choice, continuity, and data return at termination.
Transparency	Documentation the City may disclose under public records law and a commitment to provide updated system facts when material changes occur.

28. AI Inventory, Training, and Monitoring

- Information Technology and Public Relations will maintain an internal inventory of approved AI systems and significant use cases, including the owner, purpose, risk level, data category, approval conditions, vendor, renewal date, and status.
- A public summary may be issued for moderate- and high-risk systems when disclosure supports transparency and does not compromise security, privacy, procurement, or law-enforcement interests.
- Authorized users must complete role-appropriate training before operating a moderate- or high-risk system and whenever a material change alters risk or procedure.
- Business owners must report material changes, performance problems, complaints, accessibility barriers, suspected bias, security issues, and unauthorized use immediately.

29. AI Incident Response

- Stop or isolate the affected use when continued operation could create harm, spread false information, expose data, or affect a person's rights or access.
- Preserve relevant prompts, outputs, logs, screenshots, source data, approvals, vendor notices, and affected records.
- Notify Information Technology, the business owner, Public Relations, the City Manager, and the City Attorney or Human Resources when the subject requires their involvement.
- Correct public information promptly, provide an alternative service path, document affected persons and decisions, and follow applicable breach or incident notice requirements.
- Identify root cause, adjust controls, retrain users, require vendor correction, re-review the use, or retire the system before resuming operation.

PART IV

Digital Accessibility and Online Documents

A web-first standard for equal access, accessible services, and responsible use of PDFs and other files.

30. Policy Statement and Legal Standard

The City will provide public-facing web content, mobile applications, forms, documents, and digital services in a manner that gives people with disabilities equal access to City programs, services, and activities. WCAG 2.1 Level AA is the City's operational technical standard for covered web content and mobile applications.

Compliance timing

Under the current federal Title II rule, Anniston's compliance date as a public entity with fewer than 50,000 residents is April 26, 2028. The extension does not suspend the City's existing duties to provide effective communication, reasonable modifications, and equal access now.

Federal law does not ban PDF, Word, spreadsheet, or presentation files. The City's web-first policy is an operational standard designed to improve access, reduce remediation cost, and prevent fixed-format files from becoming the only doorway to a public service.

31. Web-First Rule

Simple rule for staff

If the public needs information to act, apply, pay, reserve, register, report, comment, or request service, provide the function in an accessible web-based format whenever practical—not only in a downloadable file.

- Use accessible webpage text, online forms, and approved portals as the first choice for active public information and transactions.
- Do not post a flyer, screenshot, scan, or image as the only source of essential information. Repeat the complete information in accessible webpage text.
- Do not create a new PDF form when the task can reasonably be completed through an accessible online form or service portal.
- Coordinate with Public Relations or the website administrator before posting a new public form, major document, embedded tool, or third-party service.
- Provide a prompt accessible alternative or assistance path when a platform or format cannot deliver equal access.

32. When a Fixed-Format Document May Be Used

A PDF or similar file may be appropriate when a fixed layout serves a legitimate need, including a signed record, adopted instrument, official report, bid document, archival copy, legal notice, map, print-ready material, or a document whose form must be preserved. Convenience alone is not enough when the file is the only way to access a service.

- Publish an accessible HTML summary or equivalent webpage when the document contains information the public must act on.
- Provide the accessible source format or an accessible alternative when feasible.
- Do not use an image-only scan unless it is an archival reproduction and an accessible version or assistance process is available as required.

- A document that is updated after the City's compliance date is treated as new content for this policy and must be reviewed again.

33. Accessible Document Requirements

When a public-facing PDF or office document is necessary, the department owner and publisher must ensure, to the extent applicable, that it includes:

- Real, selectable text rather than an image-only scan; accurate optical character recognition when conversion is necessary.
- A meaningful title, document language, logical heading structure, tags, reading order, and bookmarks for longer documents.
- Descriptive alternative text for informative images and appropriate treatment of decorative content.
- Tables with real header cells, simple structure, and a reading order that remains understandable with assistive technology.
- Descriptive links, legible typography, adequate color contrast, and no information conveyed by color alone.
- Form fields with labels, instructions, logical keyboard order, accessible validation, and enough time to complete the task.
- Accurate captions or transcripts for embedded audio and video and an accessible explanation of complex charts, maps, or diagrams.
- Successful accessibility review using automated checks plus human keyboard, screen-reader, zoom, reflow, and content review appropriate to the document.

34. Priority Inventory and Remediation

- 1 Stop creating new barriers: route new public forms, documents, tools, flyers, and scans through the web and accessibility review process.
- 2 Inventory active files and services: identify the owner, URL, purpose, format, posting status, public use, frequency, and whether the content is needed to obtain a service.
- 3 Prioritize high-impact content: applications, permits, payments, reservations, registrations, bids, benefits, notices, service requests, public comments, and frequently downloaded files come first.
- 4 Replace, remediate, or retire: convert active services to accessible web formats, repair necessary documents, remove duplicates, and move qualifying historic material into a clearly labeled archive.
- 5 Monitor continuously: test new content, respond to reports, reassess third-party tools, and prevent an updated file from reintroducing a barrier.

35. Limited Federal Exceptions

The Title II rule contains limited exceptions, including qualifying archived web content, certain preexisting conventional electronic documents, certain third-party content, individualized password-protected documents, and preexisting social media posts. An exception is not a blanket exemption and does not eliminate the City's broader duty to provide effective communication and equal access.

- A preexisting document exception generally does not cover a file that remains necessary to apply for, gain access to, or participate in a City service, program, or activity.

- A document changed or reposted after the compliance date may lose preexisting status.
- Third-party content posted by a City contractor or under a City arrangement generally remains the City's responsibility.
- Only the City Attorney or designated accessibility authority may approve reliance on an exception for active public content.

36. Department Responsibilities and Issue Response

Owner	Responsibility
Departments	Maintain an inventory, supply accessible source material, identify active forms and services, and correct content under their control.
Public Relations / website administrator	Publishing gate, accessible web alternatives, content standards, document review, platform coordination, and public issue routing.
Information Technology	Technical standards, procurement review, system configuration, testing support, security, and vendor remediation.
ADA Coordinator / City Attorney	Accommodation, effective-communication, exception, complaint, and legal guidance.
Vendors and contractors	Meet City accessibility requirements, provide testing evidence, correct defects, and support accessible alternatives.

Accessibility concerns must be acknowledged promptly, routed to the content owner and accessibility contact, and addressed with an accessible alternative while permanent correction is underway. Retaliation against a person requesting access or reporting a barrier is prohibited.

37. Public-Facing Web Accessibility Statement

The City of Anniston is committed to making its website and digital services accessible to all residents and visitors, including people with disabilities. The City works to ensure that website content is accessible and usable for everyone and follows WCAG 2.1 Level AA as applicable to state and local government web content.

37.1 Our commitment

The City continually works to improve the accessibility and usability of its website. Its goal is to provide digital access to City information, services, and programs in a manner that is inclusive and effective for all users. Accessibility is an ongoing effort, and the City regularly reviews website content, navigation, documents, and features.

37.2 Website accessibility features

- Clear site navigation and multiple paths to commonly used services.
- Readable text and meaningful content structure.
- Keyboard-accessible navigation where feasible.
- Alternative text for images where appropriate.
- Ongoing review of digital content and documents.

37.3 Third-party content

Some pages may link to or integrate with outside websites, applications, maps, payment systems, videos, or documents that are not fully controlled by the City. The City encourages accessibility in all third-party services and will work to provide assistance or an alternative means of access when a person reports difficulty. When a contractor or vendor provides digital content or a service for the City, the City will require accessibility appropriate to the arrangement and will not treat the contract as a transfer of the City's legal obligations.

37.4 Assistance and barrier reporting

A person who encounters a website barrier, cannot use a feature or document, or needs information in an alternative format should contact the City. When possible, the report should include the webpage or document URL, a description of the issue, the assistive technology used, and contact information for follow-up.

Accessibility assistance

Public Relations Director • 256-846-2044 • jhodes@anniston.al.gov. The City will make reasonable efforts to respond promptly and provide the information, service, or assistance through an accessible method.

The City recognizes that digital accessibility is an ongoing process and is committed to reviewing and improving its website and digital materials so residents can access City information, services, and programs more easily and effectively.

PART V

Privacy and Personal Information

Citywide standards for responsible collection, use, sharing, security, retention, individual requests, and application privacy.

38. Citywide Privacy Commitment and Scope

The City of Anniston is committed to protecting the privacy of people who interact with City programs, events, services, websites, applications, forms, and communications. This part governs how the City collects, uses, shares, secures, retains, and responds to requests concerning personal information.

Core privacy rule

Collect only information reasonably needed for an identified City purpose; limit access to authorized personnel; use and share it only for legitimate operations, safety, legal compliance, or an authorized public purpose; and retain or dispose of it according to law and the applicable records schedule.

39. Information the City May Collect

- Personal and contact information: name, address, email address, phone number, date of birth when needed for eligibility, and emergency contacts.
- Program and transaction information: registrations for programs, classes, sports, events, reservations, services, and related payment or transaction details.
- Photographs and video: images recorded at City events, activities, classes, facilities, or programs for authorized promotional, informational, historical, or archival purposes.
- Special categories: medical or allergy information needed for participant safety and parent or guardian information for programs involving minors.
- Digital and device information: device type, operating system, application usage, service interactions, and other technical information reasonably needed to operate, secure, evaluate, or improve a City service.

40. How the City Uses Information

- Administer City programs, events, registrations, classes, payments, facilities, and services.
- Send confirmations, schedules, reminders, changes, safety information, and other service-related communications.
- Protect the safety and well-being of participants, particularly children and people with identified medical or allergy needs.
- Improve the functionality, accessibility, security, and user experience of City websites, applications, and services.
- Promote City programs and services through authorized social media, brochures, websites, news releases, and other public-information materials.
- Meet legal, financial, records, public-safety, audit, and operational requirements.

41. Information Sharing and No-Sale Rule

The City shares personal information only when reasonably necessary for an authorized purpose and only with people or entities that need it to perform that purpose.

- Relevant City departments may access information needed to provide a service or administer a program.

- Authorized service providers may receive information needed for payment processing, registration, program administration, event management, hosting, security, or another contracted function.
- Information may be disclosed when required by law, legal process, court order, public-records obligations, audit, or a legitimate public-safety need.
- Approved photographs and video may be used for public relations, marketing, event promotion, public information, and archival purposes subject to the notice, permission, and opt-out rules below.
- The City does not sell, rent, or lease personal information to third parties.

42. Photographs, Video, and Promotional Use

People attending public City events or programs may appear incidentally in photographs or video used for authorized City communication. A person who does not want their image used should notify the City at registration, inform event staff when practical, or contact the City at 256-236-3422 or jhodes@anniston1.gov.

- The City will honor reasonable and practical requests to avoid or remove a person's image from promotional materials, subject to legal, records, archival, operational, and already-distributed material limitations.
- Planned, featured, testimonial, or individually identifiable promotional use should receive an appropriate release when required by City procedure.
- Images must be used with dignity and in a manner consistent with the event, permission, public context, and the Social Media Policy.

43. Children's Privacy

Information collected for a child under thirteen is provided by a parent or guardian. The City uses children's information only for authorized program administration, eligibility, payment, communication, safety, records, or another lawful purpose. Planned promotional photographs or video of children require appropriate parent or guardian permission under City procedure.

- Collect only information reasonably necessary for the program and safety of the child.
- Restrict access to employees and providers with a legitimate need to know.
- Do not pair a child's full name with a home address, routine schedule, school, or other information that creates avoidable safety risk.
- The Parks and Recreation application obtains information for minors through a parent or guardian and follows the children's privacy requirements stated in its application policy.

44. Data Security, Retention, and Incident Response

- Restrict sensitive information to authorized personnel and apply least-privilege access.
- Use secure storage for digital and physical records, encrypted transmission for online payments where applicable, and regular system or vulnerability review.
- Do not place personal, payment, medical, child, or other sensitive information in an unapproved platform, AI system, personal account, or unsecured communication channel.
- Retain information according to the Alabama records schedule, City procedure, contract requirements, and legal holds; securely dispose of information when authorized.

- Report suspected loss, unauthorized access, disclosure, alteration, fraud, or misuse immediately to Information Technology and the responsible department, with escalation to the City Manager, Public Relations, Risk Management, or City Attorney as appropriate.

45. Access, Correction, Removal, and Deletion Requests

Subject to identity verification and applicable law, records schedules, public-records requirements, legal holds, contracts, and operational needs, a person may request to:

- Access personal information the City maintains about them; a public-records or department request may be required.
- Correct or update inaccurate personal information.
- Request reasonable and practical removal of their photograph or video from promotional materials.
- Request deletion of personal information when the City is not legally or operationally required to retain it.

Citywide privacy contact

City of Anniston • jhodes@anniston.al.gov • 256-236-3422. The request will be routed to the department, records officer, Information Technology, legal counsel, or service provider needed to evaluate and respond.

46. Third-Party Services, Policy Changes, and Accountability

- Departments must review a provider's privacy, security, accessibility, records, ownership, retention, breach-notice, deletion, and subcontractor terms before use.
- The City will require appropriate privacy and security obligations in contracts and will not represent that a vendor's independent practices are under direct City control when they are not.
- Users should review the privacy notice of an independent third-party site before providing information outside a City-controlled service.
- Material changes to a City privacy practice must be coordinated with Public Relations, Information Technology, the affected department, records staff, Purchasing, and the City Attorney as appropriate, then published on the City website and applicable application listing.

47. Parks and Recreation Application Privacy Addendum

The Anniston Parks and Recreation application supports registration for sports and classes, online payment, and enrollment in community-center activities. This addendum applies in addition to the Citywide privacy requirements above.

47.1 Application information and use

- The application may collect names, contact information, payment information, birth dates for child registration, emergency contacts, device type, operating system, application usage, registration history, and payment transaction details.
- The information is used to complete registrations and payments, send confirmations and reminders, improve functionality and user experience, meet legal requirements, and protect user safety.

47.2 Sharing, advertising, and security

- Information may be shared with trusted payment processors, relevant City departments, and law enforcement or other authorities when required by law. It is not sold, rented, or leased.
- The application does not display banner, interstitial, native, or other advertising.
- The City uses encrypted transmission for payment activity where applicable, monitors for vulnerabilities, and restricts sensitive data to authorized personnel.

47.3 User choices, children, and outside links

- Users may request access, correction, or deletion subject to legal and operational obligations.
- Information for minors is provided by a parent or guardian and handled under the children's privacy requirements above.
- The application may link to outside services for payment or additional information. Users should review the outside provider's privacy policy before submitting information.

Parks and Recreation application contact
City of Anniston Parks and Recreation Department • fburroughs@anniston.al.gov •
256-236-8221. The privacy policy must remain available in the application store listing, within
the application, and on the City website.

PART VI

Film Coordination and Permit Intake

A clear, content-neutral process for productions using City property, services, streets, facilities, or public-safety resources.

48. Purpose and Administrative Status

The City welcomes responsible film, television, commercial, documentary, music-video, and similar production activity that supports economic development while protecting public safety, public access, neighborhoods, City property, and continuity of municipal services.

Authority boundary

This part establishes the City's administrative intake and coordination process. It does not create a criminal offense, civil penalty, application fee, or deposit requirement that lacks authority under adopted law, an approved fee schedule, a contract, or lawful property-use conditions. Any requirement dependent on City Council action becomes enforceable only after that action occurs.

49. When City Coordination Is Required

A production should submit the City's Film Permit Application when it requests use of City property, streets, sidewalks, parks, facilities, equipment, personnel, traffic control, public-safety support, special effects review, exclusive access, parking control, or another City service or accommodation.

- Private-property filming that does not affect public areas, City services, traffic, noise, safety, or surrounding property ordinarily does not require City film coordination.
- Routine personal filming and bona fide news gathering ordinarily do not require a film permit. This manual does not restrict lawful recording in public places or condition news coverage on government approval.
- A production remains responsible for permits, licenses, permissions, releases, property rights, aviation rules, labor rules, copyright, and other legal requirements outside this process.

50. Lead Office and Submission Timing

The City Manager's Office receives the application. The Public Relations Department serves as the production liaison and coordinates review with affected departments. The City Clerk maintains the official record as required.

- Low-impact production: submit a complete application at least five business days before filming.
- High-impact production: submit at least fourteen calendar days before filming when the project involves a street closure, special effects, significant noise, a large crew, neighborhood disruption, City personnel, public-safety resources, complex insurance review, or multiple affected locations.
- Incomplete applications do not begin the review period. Late requests may be declined when the City cannot complete a safe and responsible review.

51. Application Requirements

A complete submission includes information sufficient to understand the production and its public impact:

- Production title, type, company, primary contact, contact information, and responsible on-site representative.
- Each location, filming date, start and end time, base camp, crew parking, expected crew and vehicle count, equipment, and requested City services.
- A clear description of filming activity, production subject, lighting, generators, noise, drones, animals, weapons, stunts, smoke, pyrotechnics, explosions, special effects, or other unusual conditions.

- Traffic, pedestrian, parking, accessibility, crowd, emergency-access, and public-safety plans when applicable.
- Proof of required property permission, insurance, neighborhood or business notice, Fire Department approval, and other supporting documents.
- The intended use of footage involving members of the public, personal property, City facilities, or planned participation by City personnel, including releases or compensation where applicable.

52. Impact Classification

Class	Indicators	Typical review
Low impact	Small crew; ordinary equipment; no closure, effects, exclusive access, City services, or material noise; minimal public disruption.	Public Relations and property owner/department; City Manager approval as required.
High impact	Closures, traffic control, special effects, stunts, weapons, drones, amplified noise, large footprint, nighttime activity, neighborhood impact, emergency resources, or exclusive City-property use.	City Manager plus Public Relations and all affected departments; Fire, Police, Public Works, Risk, Legal, or others as needed.

53. Review and Decision Process

- 1 Intake: Staff date-stamp the application, check completeness, identify affected property and departments, and classify the impact.
- 2 Department review: Public Relations circulates the request to City Manager, Police, Fire, Public Works, Parks and Recreation, Risk Management, City Attorney, Engineering, or other offices as needed.
- 3 Conditions and cost: Departments identify safety requirements, service availability, staffing, traffic measures, accessibility, restoration, insurance, deposits, and direct City costs that may lawfully apply.
- 4 Decision: The approving authority issues written approval, approval with conditions, a request for additional information, or denial based on documented operational, safety, property, legal, or resource grounds.
- 5 Pre-production conference: High-impact productions meet with affected City representatives before filming and receive final contact and incident instructions.
- 6 Closeout: Staff document completion, property condition, reimbursable services, incidents, complaints, and release of any authorized security after obligations are satisfied.

Content-neutral administration

A decision may not be based on agreement or disagreement with a production's message, viewpoint, subject, speakers, or anticipated audience. Conditions must address legitimate operational, safety, property, legal, or resource impacts.

54. Insurance, Deposits, Fees, and City Services

- The current application requests evidence of general liability coverage and may require automobile or workers' compensation coverage as applicable. Coverage limits, additional-insured language, and waivers are determined by the City's authorized risk and legal reviewers.

- A fee, deposit, bond, reimbursement, or service charge is collected only when supported by adopted authority, an approved schedule, a lawful contract, or conditions governing use of City property or services.
- Police, Fire, Public Works, facility, traffic-control, cleanup, utility, or other direct costs may be charged when lawfully authorized and disclosed to the applicant before final approval.
- City-commissioned productions may receive approved waivers or alternative arrangements consistent with law and City policy.

55. Public Safety, Neighborhoods, and Accessibility

- Emergency access, accessible routes, sidewalks, building entrances, transit stops, fire lanes, hydrants, and required parking access must remain available unless an approved plan provides an equivalent safe route.
- Street or lane closures require an approved traffic-control plan and the authority of the responsible City department. A production may not direct public traffic without authorization.
- Special effects, pyrotechnics, smoke, open flame, simulated weapons, stunts, or hazardous activity require advance review and all legally required approvals.
- Affected residents and businesses must receive notice when required by the approved conditions. Notice should identify the location, hours, expected impact, production contact, and City contact.
- The permittee must control noise, lighting, trash, parking, generators, cables, trip hazards, and crowd impacts and restore City property to its prior condition.

56. Filming City Employees and Facilities

Lawful recording of public employees performing public duties in a public place is not prohibited merely because consent was not obtained. Recording may not materially interfere with duties, cross a lawful safety perimeter, enter a non-public area, compromise protected information, or create a safety hazard.

- Planned participation by an employee in a City-endorsed or coordinated production requires supervisor and Public Relations approval and any required release.
- Non-public offices, locker rooms, restricted infrastructure, private meetings, records areas, secure operations, and locations where a person has a reasonable expectation of privacy may not be filmed without authorization.
- Emergency scenes and active operations remain under incident command. Production access may be restricted to protect life, safety, evidence, privacy, and continuity of service.
- The City may require a location agreement, escort, credit language, brand conditions, or limits on seals, uniforms, vehicles, and identifiable facilities where necessary to avoid false endorsement or security risk.

57. Compliance, Revocation, and Records

Approval may be suspended or revoked when a production materially departs from its approved activity, violates lawful conditions, creates an unapproved safety hazard, interferes with City operations, fails to maintain required insurance, or refuses a lawful direction relating to City property or services. Staff should document the reason, action taken, and available correction path.

Applications, approvals, denials, conditions, plans, insurance records, correspondence, cost records, complaints, incident reports, photographs, and closeout records must be retained according to the applicable records schedule and any legal hold.

Appendix E

AI Use-Case Intake Checklist

- Define the public or operational need, intended outcome, current process, and alternatives considered.
- Identify the business owner, accountable employee, users, affected people, vendor, integrations, and expected cost.
- Describe inputs, outputs, personal or sensitive data, data location, retention, sharing, deletion, and model-training use.
- Identify whether a person can opt out, obtain human review, understand the result, correct an error, appeal an effect, and access an equivalent non-AI service.
- Assess severity, duration, reversibility, accuracy, bias, accessibility, cybersecurity, public-records, procurement, and reputational risk.
- Define testing, approval, training, notice, monitoring, performance metrics, incident response, fallback, shutdown, and retirement.

Appendix F

AI Output Release Checklist

Check	Release requirement
Source verification	All facts, names, dates, amounts, quotes, citations, links, and legal assertions match authoritative sources.
Authenticity	Nothing fabricated or altered could be mistaken for a real event, person, statement, condition, or City action.
Privacy and security	No confidential, protected, personal, credential, or security-sensitive information is exposed.
Bias and dignity	Content is checked for stereotyping, unequal treatment, offensive material, and foreseeable harm.
Accessibility	Text, visuals, captions, reading order, contrast, links, and alternative formats meet City standards.
Approval and records	Responsible human reviewer and required City approvers are identified; necessary records are preserved.

Appendix G

Accessible Publishing Checklist

- Can the public complete the task through an accessible webpage, form, or portal instead of relying only on a file?
- Is all essential flyer, image, map, audio, and video information also available as accessible text?
- If a document is necessary, does it have selectable text, tags, headings, language, title, reading order, bookmarks, alt text, accessible tables, descriptive links, and sufficient contrast?
- Can forms be completed by keyboard and assistive technology, with clear labels, instructions, validation, and error recovery?
- Were automated checks followed by human keyboard, zoom, reflow, content, and assistive-technology review appropriate to the content?
- Is an accessible alternative and a clear assistance contact available if a known barrier remains?

Appendix H

Film Application Review Checklist

- Application is complete; correct location owner and approving authority are identified.
- Impact is classified; lead time is sufficient; all affected departments have reviewed.
- Property permission, insurance, traffic plan, Fire approval, resident/business notice, accessibility plan, and service requests are complete as applicable.
- Conditions are content-neutral, within City authority, written clearly, and tied to safety, access, property, operations, law, or resources.
- Any fee, deposit, reimbursement, or insurance requirement has lawful authority and was disclosed before approval.
- Production and City contacts, incident process, restoration standard, closeout steps, and records retention are documented.

Appendix I

Privacy Request and Review Checklist

- Record the requester's name, contact information, requested action, affected service or program, and the information or image at issue; verify identity before releasing or changing personal information.
- Identify the responsible department, system owner, records custodian, service provider, and any other location where responsive information may be held.
- Check the applicable records schedule, public-records requirements, litigation or legal hold, contract terms, financial requirements, and operational need before approving deletion.
- Determine whether the request seeks access, correction, an update, practical removal of a promotional image, deletion, or an accessible alternative; define the scope and search performed.
- Coordinate with Information Technology, Public Relations, Parks and Recreation, the City Clerk, the City Attorney, or the vendor when their systems, records, or legal responsibilities are involved.
- Respond through a secure and accessible method, explain any limitation, document the decision and actions taken, and preserve the request and response under the applicable records schedule.

Appendix J

Authorities and Reference Standards

1. U.S. Department of Justice - Title II Web and Mobile Accessibility Rule Fact Sheet
<https://www.ada.gov/resources/2024-03-08-web-rule/>
2. U.S. Department of Justice - First Steps Toward Compliance
<https://www.ada.gov/resources/web-rule-first-steps/>
3. U.S. Department of Justice - 2026 Interim Final Rule Extending Compliance Dates
<https://www.ada.gov/assets/pdfs/2026-ifr.pdf>
4. WCAG 2.1
<https://www.w3.org/TR/WCAG21/>
5. NIST Artificial Intelligence Risk Management Framework
<https://www.nist.gov/itl/ai-risk-management-framework>
6. NIST Generative AI Profile
<https://nvlpubs.nist.gov/nistpubs/ai/NIST.AI.600-1.pdf>
7. GovAI Coalition - AI Governance Handbook
<https://www.sanjoseca.gov/your-government/departments-offices/information-technology/artificial-intelligence>
8. City of Anniston - Web Accessibility Statement
<https://anniston.al.gov/web-accessibility/>
9. City of Anniston - Privacy Policies
<https://anniston.al.gov/communications/privacy-policies>
10. City of Anniston - Citywide Privacy Policy
<https://anniston.al.gov/wp-content/uploads/2024/12/Privacy-Policy-City-of-Anniston-Alabama.pdf>
11. City of Anniston - Parks and Recreation Application Privacy Policy
<https://anniston.al.gov/wp-content/uploads/2024/12/Privacy-Policy-for-Anniston-Parks-and-Recreation-App.pdf>
12. City of Anniston
<https://www.anniston.al.gov/>

This manual also incorporates the City's Social Media Policy, Artificial Intelligence Use Policy for City Communications and Media, Digital Accessibility and Online Document Policy, public Web Accessibility Statement, Citywide Privacy Policy, Parks and Recreation Application Privacy Policy, Film Permit Application, and film-permitting process materials supplied for administrative development.