ALBANY COUNTY FIRE DISTRICT #1

Data Privacy Policy

Privacy Notice

This document is an internal privacy policy governing how Albany County Fire District #1 ("District") personnel collect, handle, and protect personal data to comply with Wyoming law. It is not a public-facing privacy notice. Entities that collect personal data directly from members of the public through a website, online portal, or public service application are considered separately, pursuant to and under law.

Section 1 — Purpose and Scope

Statement 1.1. This policy establishes requirements for the District regarding the collection, access, retention, security, and use of personal data in accordance with Wyoming Statute § 9-21-201 through § 9-21-203. This policy is intended to protect the privacy rights of Wyoming residents while enabling the District to fulfill its lawful governmental functions.

Statement 1.2. This policy applies to all operating units and programs of the District and to all personnel who collect, access, retain, use, or transfer personal data in the performance of their official duties. This includes full-time, part-time, temporary, and seasonal employees, elected officials, appointed officials, and volunteers. It also applies to contractors, consultants, and third-party vendors who receive or access personal data of the District pursuant to a government services contract.

Statement 1.3. ***Excluded Functions.*** Consistent with the Data Privacy in Government Entities Act, W.S. § 9-21-201(a)(ii), this policy does not apply to the judicial branch of government or to any law enforcement agency as defined in W.S. § 9-21-201(a)(iv). To the extent the District is alongside any agency primarily focused on crime prevention/investigation or enforcing penal, traffic, or regulatory laws, this policy shall not apply.

Statement 1.4. All records created or received by the District in the conduct of public business are public records as defined by W.S. § 9-2-401(a)(v) and are presumptively open for public inspection under the Wyoming Public Records Act, W.S. § 16-4-202 or the District's Public Records Policy. Nothing in this policy alters or limits that right of inspection. This policy governs the responsible handling of personal data within that broader public records universe.

Statement 1.5. To the extent any provision of this policy conflicts with applicable federal law, the federal law controls. Where the District is subject to a federal data governance framework governing the collection, retention, access, transfer, or handling of specific categories of data, compliance with that framework satisfies this policy's requirements for the data and conduct it governs.

DRAFT

Section 2 — Definitions

Statement 2.1. ***Privacy Contact.*** The District designates one individual as the Privacy Contact to serve as the primary point of contact for personal data access requests, written objections, exemption documentation, and policy compliance matters under this policy. The Privacy Contact shall be the District Chair.

Statement 2.2. ***Deidentified Data.*** Data which cannot reasonably be used to infer information about, or otherwise be linked to, an identified or identifiable natural person or personal digital identity, or a device linked to a natural person or personal digital identity. Deidentified data is not subject to the requirements of this policy.

Statement 2.3. ***Government Entity.*** The state and all its political subdivisions, agencies, instrumentalities, and institutions, and any local government entity. This includes the District.

Statement 2.4. ***Law Enforcement Agency.*** A county, municipal, college or university police force, the Wyoming Highway Patrol, the Division of Criminal Investigation, the Department of Corrections, the Game and Fish Department when acting within its law enforcement capacity, or any state or local agency or political subdivision, or part thereof, to the extent that the primary purpose of the agency or subdivision is the prevention or investigation of crime or the enforcement of penal, traffic, regulatory, or criminal laws.

Statement 2.5. ***Identified or Identifiable Natural Person.*** A natural person who can be readily identified, directly or indirectly, by reference to an identifier such as a name, an identification number, specific geolocation data, or an online identifier.

Statement 2.6. ***Identification Number.*** Any numeric, alphanumeric, or other coded value assigned to uniquely identify a natural person within a recordkeeping system, whether government-issued or program-specific. This includes, but is not limited to, social security numbers, driver's license numbers, state-issued ID numbers, taxpayer identification numbers, and agency- or program-assigned case numbers, client IDs, or participant identifiers. A program-specific identifier that links records to a specific individual within a system constitutes an identification number for purposes of this definition regardless of whether it is used outside that system.

Statement 2.7. ***Geolocation Data (Specific).*** Data that describes or can be used to infer the geographic location of a natural person or a device associated with a natural person, including coordinates, addresses, GPS data, cell-tower data, and IP-derived location. For purposes of this policy, "specific geolocation data" includes both static location data (e.g., a home or work address) and dynamic or transient location data (e.g., movement records or timestamped location logs). Dynamic location data that requires a temporal variable to identify a person remains personal data subject to this policy.

Statement 2.8. ***Online Identifier.*** An identifier assigned to a device, application, account, or user session during online activity that can be used, alone or in combination with other data, to identify a natural person directly or indirectly. Examples include, but are not limited to: IP addresses, cookie identifiers, browser fingerprints, device identifiers, advertising identifiers (e.g., IDFA, GAID), session tokens, and account usernames linked to a real identity.

Statement 2.9. ***Personal Data.*** Information that is linked or reasonably linkable to an identified or identifiable natural person or personal digital identity, and that does not include deidentified data.

DRAFT

Statement 2.10. ***Personal Digital Identity.*** As defined in W.S. § 8-1-102(a)(xviii): the unique, authenticatable, and verifiable digital identity of a natural person. Personal digital identity is included within the definition of personal data for purposes of this policy.

Statement 2.11. ***Political Subdivision.*** A county, municipality, special district, or other local government entity, including the District.

Statement 2.12. ***Public Record (Records Management Act).*** Includes the original and all copies of any paper, correspondence, form, book, photograph, photostat, film, microfilm, scan, sound recording, map, drawing, or other document, regardless of physical, digital, or electronic form or characteristics, which have been made or received in transacting public business by the District.

Statement 2.13. ***Public Records (Wyoming Public Records Act).*** Includes any information in a physical form created, accepted, or obtained by the District in furtherance of its official function and transaction of public business which is not privileged or confidential by law. Without limiting the foregoing, includes any written communication or other information, whether in paper, electronic, or other physical form, received by a governmental entity in furtherance of the transaction of public business, whether at a meeting or outside a meeting.

Statement 2.14. ***Retention Schedule.*** A document that identifies categories of public records, specifies how long each category must be retained, and authorizes the disposition of records at the end of that period, including but not limited to the schedule set-forth pursuant to the District's Retention Record Policy.

Statement 2.15. ***District Chair.*** The individual holding primary administrative authority over the District's day-to-day operations and staff, as may be designated to the District's Operations Chief or other.

Section 3 —Governing Framework

Statement 3.1. This policy is the District's primary governing policy on personal data. No program, function, or personnel of the District may adopt a practice, procedure, or informal standard that reduces the protections required by this policy. Program-level procedures that augment these protections are permitted.

Statement 3.2. Where a specific program or function of the District is subject to HIPAA or FERPA, compliance with Statement 4.6 satisfies the requirements of Sections 5 and 6 of this policy for personal data regulated under those acts.

Section 4 — Statutory Exemptions and Safe Harbors

Statement 4.1. All records created or received by the District in the conduct of public business are public records as defined by the Records Management Act and are presumptively open for public inspection under the Wyoming Public Records Act and the District's Public Records Policy.

Statement 4.2. ***What this policy covers.*** This policy governs the responsible handling of personal data as defined by the Data Privacy in Government Entities Act, including information linked or reasonably linkable to an identified or identifiable natural person or personal digital identity, regardless of whether the record containing that data is open to or exempt from public inspection under the Wyoming Public Records

DRAFT

Act or the District's Public Record Policy. Covered records include, but are not limited to, medical, psychological, and personnel records that may be withheld from inspection under the Wyoming Public Records Act or the District's Public Record Policy.

Statement 4.3. ***What this policy does not cover.*** Deidentified data as defined by the Data Privacy in Government Entities Act is not subject to this policy. This policy does not apply to the judicial branch or to law enforcement agencies as defined by the Data Privacy in Government Entities Act. Entities subject to HIPAA or FERPA that maintain a compliant written data collection and retention policy are deemed compliant with Statement 4.6. Individual data subject rights requests by Wyoming residents are governed by Section 7 of this policy.

Statement 4.4. To the extent any provision of this policy conflicts with any other applicable state or federal law, the other law controls.

Statement 4.5. Nothing in this policy abrogates any disclosure obligation of the District under the Wyoming Public Records Act or the District's Public Records Policy. If personal data in the possession of the District is required to be disclosed in response to a public records request under W.S. § 16-4-202, it shall be disclosed consistent with the requirements of the Wyoming Public Records Act, W.S. § 9-21-201 through § 9-21-203, and the District's Public Records Policy.

Statement 4.6. Any District departments that are subject to HIPAA or FERPA and are compliant with a written data collection and retention policy meeting the requirements of HIPAA or FERPA shall be deemed compliant with Sections 5 and 6 of this policy for personal data regulated under those acts. T

Statement 4.7. A department of the District that cannot achieve full technical compliance with any provision of this policy due to an existing system or technology limitation shall not be found in violation of this policy, provided that:

(a) the specific limitation has been documented in writing;

(b) a remediation path has been identified and submitted to the District Chair; and

(c) all compensating controls available within current means have been implemented.

Statement 4.8. Consistent with Statement 4.4, District departments subject to federal data governance frameworks governing the collection, retention, access, transfer, or handling of specific categories of data, including but not limited to Internal Revenue Code § 6103 and IRS Publication 1075 (Federal Tax Information), the Privacy Act of 1974, 5 U.S.C. § 552a, and other federally mandated data governance requirements, shall comply with those frameworks directly.

Section 5 — Personal Data Collection and Retention

Statement 5.1. The District shall only collect and maintain personal data that is reasonably necessary for the performance of its lawful governmental functions. Each type of personal data collected must be necessary for a specific, identifiable governmental function.

Statement 5.2. The District shall not retain personal data for longer than three (3) years without a written policy identifying the extended retention period and providing a reasonable justification for the extension.

DRAFT

Statutory retention requirements established under Wyoming law constitute reasonable justification for any extended retention period.

Statement 5.3. District departments subject to HIPAA or FERPA that maintain a written data collection and retention policy compliant with those acts are deemed in compliance with this Section 5 for data regulated under those acts. See Section 4, Statement 4.6, for full requirements.

Section 6 — Personal Data Transfer and Disclosure

Statement 6.1. The District shall not purchase, sell, trade, or transfer personal data without the express written consent of the natural person whom the personal data references, except as expressly provided by law or as permitted under Statements 6.2 through 6.5 of this policy.

Statement 6.2. The District may transfer personal data to another government entity provided that the receiving government entity complies with Wyoming Statute § 9-21-201 through § 9-21-203. Prior to any such transfer, the District shall document the transfer, the receiving entity, the legal basis, and the purpose.

Statement 6.3. The District may transfer personal data to a non-government entity contracted to provide or assist with government services, subject to all of the following:

(a) any contract must include provisions requiring the protection of personal data consistent with W.S. § 9-21-201 through § 9-21-203;

(b) any personal data transferred must be returned or destroyed by the contractor once no longer necessary for the contracted service; and

(c) no contractor shall maintain, sell, transfer, process, or otherwise use personal data in any manner except as necessary to provide the contracted service.

Statement 6.4. The District may transfer personal data where such transfer is permitted or required by HIPAA (45 CFR Part 164), FERPA (34 CFR Part 99), or any other applicable federal law governing the transfer, including, for example, IRC § 6103 and IRS Publication 1075 (Federal Tax Information), the Privacy Act of 1974 (5 U.S.C. § 552a), 42 CFR Part 2, the Driver's Privacy Protection Act (18 U.S.C. § 2721), Social Security Act § 1106 (42 U.S.C. § 1306), Title IV-D (42 U.S.C. § 654), and the FBI CJIS Security Policy / 28 CFR Part 20.

Statement 6.5. Transfers of personal data not otherwise authorized by this policy require a written exception approved by a majority of the District's elected governing members. Exception requests must:

(a) be submitted in writing;

(b) be evaluated on a case-by-case basis;

(c) receive public written approval by the governing body; and

(d) not exceed a term of two (2) years per petition. All approved exceptions shall be made publicly available.

DRAFT

Section 7 — Individual Rights

Statement 7.1. Any current or former Wyoming resident, or their legally authorized representative, may request a copy of their personal data from the District under W.S. § 9-21-202(b). The District may charge a fee for production of the requested personal data, provided that any such fee is authorized by a duly enacted resolution, ordinance, or other lawful authority of the governing body, and is reasonable and consistent with the fee standards of the Wyoming Public Records Act (W.S. § 16-4-204) and the District's Public Records Policy.

Statement 7.2. A current or former Wyoming resident, or their legally authorized representative, may submit a written request to the District to access personal data about themselves that the District maintains. The District shall respond within the timeframe established and published by the District pursuant to this policy.

Statement 7.3. Before releasing personal data in response to a request under Statement 7.1, the District shall take reasonable steps to verify the identity of the requestor. Verification shall be proportionate to the sensitivity of the data requested and may include one or more of the following: (a) a copy of a government-issued photo identification; (b) confirmation of an account number, case number, or other identifier known only to the data subject and the District; or (c) any other method reasonably calculated to confirm the requestor is the individual whose data is being requested. Where a request is filed by a legally authorized representative, the District shall also verify the representative's legal authority before releasing personal data. If identity or authority cannot be reasonably confirmed, the District may delay the response and request additional documentation. The District shall not release personal data where identity verification has failed or been refused.

Statement 7.4. A current or former Wyoming resident, or their legally authorized representative, who objects to the accuracy, completeness, pertinence, timeliness, relevance, retention, dissemination, or denial of access to their personal data maintained by the District may file a written objection with the District.

Statement 7.5. Upon receipt of a written objection under Statement 7.4, the District shall, within sixty (60) calendar days (the sixty-day deadline is statutory and cannot be extended):

(a) verify the identity of the individual or their legally authorized representative who filed the objection;

(b) review the validity of the objection;

(c) if the objection is meritorious, alter the contents, holding methods, dissemination, or use of the personal data, or delete or grant access to it;

(d) if the objection lacks merit, provide the individual the opportunity to have a statement reflecting their views maintained with the personal data; and

(e) notify the individual in writing of any decision regarding the objection.

Statement 7.6. Individuals who are not current or former Wyoming residents do not have standing to exercise the rights in Statements 7.1 through 7.4 under W.S. § 9-21-202(b) and (c). Such individuals may request access to agency-held records pursuant to the Wyoming Public Records Act (W.S. § 16-4-201 through § 16-4-205), subject to applicable exemptions and the procedures governing public records requests and the District's Public Record Policy.

DRAFT

Statement 7.7. The District shall designate a contact for personal data access requests and written objections. The designated contact shall be the District Chair or another staff member designated by the District Chair and all current contact information shall be found on the District's website.

Section 8 — Data Security

Statement 8.1. All personnel with access to personal data shall receive orientation on this policy and their obligations under it prior to or promptly upon receiving such access. At a minimum, this orientation shall communicate the definition of personal data under this policy, the permitted purposes for which personal data may be used, the requirement to report suspected unauthorized access or disclosure, and the consequences of policy violations.

Statement 8.2. In the event of an actual or suspected breach of personal data, the District shall follow its incident response procedures and comply with all applicable state and federal breach notification requirements.

Statement 8.3. The District shall implement access controls ensuring that personal data is accessible only to personnel with a legitimate need in the performance of their official duties. Access privileges shall be reviewed at least annually and promptly revoked upon separation or reassignment.

Statement 8.4. The District shall maintain documentation of security measures implemented under this section, including access control records, training records, and security incident reports.

Statement 8.5. When procuring, developing, or significantly upgrading information systems, software, or applications that will process personal data, the District may require that privacy and security controls be identified and documented as part of procurement specifications or project requirements prior to system deployment.

Section 9 — Compliance and Enforcement

Statement 9.1. All District personnel subject to this policy, including elected members, employees, contractors, temporary workers, and volunteers, are responsible for understanding and complying with this policy. Failure to comply may result in disciplinary action up to and including termination of employment or contract or volunteer association, consistent with the District's personnel policies and applicable law.

Statement 9.2. Contractors and vendors who fail to comply with the personal data protection requirements of their service contracts with the District shall be subject to remedies available under the contract, which shall include at minimum: suspension or termination of the contract; immediate revocation of access to District systems and data; and a requirement to return or certify destruction of all personal data in their possession. Contractor obligations are established in Statement 6.3 and Appendix A.

Statement 9.3. Any District personnel who know of or reasonably suspect a violation of this policy, including unauthorized access, use, transfer, or disclosure of personal data, shall report the matter promptly to their direct supervisor and to the District Chair. Anonymous reports shall be accepted by both the District Chair and President of the elected members of the District. Reports shall not result in retaliation against the

DRAFT

reporting individual. The District Chair shall log all reports, investigate or escalate as appropriate, and document findings and any corrective action taken.

Statement 9.4. Upon a confirmed violation of this policy, the District shall:

(a) take prompt corrective action to stop or remedy the violation;

(b) assess whether the violation constitutes a data breach requiring notification under applicable federal law or the District's incident response procedures, and comply accordingly;

(c) assess whether any Wyoming Public Records Act disclosure obligation was violated;

(d) document the violation, the corrective action taken, and any notifications made; and

(e) determine whether a policy amendment or additional training is required to prevent recurrence.

Statement 9.5. This policy shall be reviewed at least annually by the District Chair and legal counsel. An out-of-cycle review shall be conducted whenever any of the following occurs: (a) a material change in applicable state or federal law affecting personal data; (b) a confirmed policy violation resulting in a finding that a policy provision is unclear or inadequate; (c) a significant new personal data collection activity not addressed by the current data inventory; or (d) a directive from the District's elected members requiring review. Material amendments require approval by the District's elected members. All reviews shall be documented.

Statement 9.6. A department of the District that cannot achieve full technical compliance with any provision of this policy due to a documented system or technology limitation shall not be found in violation of this policy under the conditions established in Statement 4.7.

Section 10 — Exception Process

The following process applies to transfer exceptions under Statement 6.5 (W.S. § 9-21-202(a)(iii)):

Statement 10.1. The requesting department prepares a written exception request identifying the personal data involved, the proposed recipient, the purpose, and the duration requested (not to exceed two years).

Statement 10.2. The request is submitted to the District Chair for initial review.

Statement 10.3. The exception request is placed on the agenda of the District's elected members' public meeting for consideration and action.

Statement 10.4. If approved, the governing body's written approval is made publicly available (e.g., meeting minutes, District website, public records) and retained by the District Chair.

Statement 10.5. Each approved exception is valid for a maximum of two (2) years. Renewal requires a new petition and governing body approval.

DRAFT

Appendix A — Required Vendor / Contractor Data Protection Contract Language

The following language shall be incorporated into all contracts with nongovernment entities involving access to or transfer of personal data, consistent with W.S. § 9-21-202(a)(ii). It may be included as a standalone addendum or inserted directly into the main contract body.

Personal Data Protection Addendum

This addendum (the "*Agreement Title or Number* — Personal Data Protection Addendum") is incorporated into and made part of the agreement between Albany County Fire District #1 ("Entity") and *[Contractor Name]* ("Contractor") dated *[Date]*, and controls over any conflicting provision of the main agreement on matters of personal data protection.

1. Compliance Obligation. Contractor shall protect all personal data (as defined in W.S. § 9-21-201(a)(v)) received from or on behalf of Entity in a manner consistent with Wyoming Statute § 9-21-201 through § 9-21-203 and Entity's Data Privacy Policy, as amended from time to time.

2. Permitted Use. Contractor shall not maintain, sell, transfer, process, or otherwise use personal data in any manner except as strictly necessary to perform the contracted services. If Contractor is required by court order, subpoena, or applicable law to disclose personal data, Contractor shall: (a) notify Entity in writing immediately upon receipt of such order or process, unless prohibited by law from doing so; (b) cooperate with Entity's efforts to seek a protective order or other appropriate relief; and (c) disclose only that portion of personal data legally required.

3. Return or Destruction. Upon completion or termination of the agreement, or when personal data is no longer necessary for the contracted service, Contractor shall promptly return or destroy all personal data in accordance with Entity's written instructions and shall provide written certification of such return or destruction within thirty (30) days.

4. No Secondary Disclosure. Contractor shall not transfer, sell, or disclose personal data to any third party without prior written approval of Entity, except as required by court order, subpoena, or applicable law, in which case the notice and cooperation requirements of Clause 2 apply.

5. Security Safeguards. Contractor shall implement and maintain administrative, technical, and physical safeguards appropriate to the nature, volume, and sensitivity of the personal data received, designed to protect against unauthorized access, use, disclosure, modification, or destruction. Upon request by Entity, Contractor shall provide reasonable written evidence of its security controls, policies, or certifications within thirty (30) days of the request.

6. Personnel Training. Contractor shall ensure that all personnel who access or handle personal data received from Entity have received appropriate data protection training prior to accessing such data, and annually thereafter. Contractor shall certify compliance with this requirement upon Entity's request.

DRAFT

7. Breach Notification and Response. Contractor shall notify Entity in writing within forty-eight (48) hours of discovering any actual or suspected unauthorized access, use, disclosure, modification, or destruction of personal data. Contractor shall: (a) provide all information reasonably required by Entity to assess the nature and scope of the incident; (b) cooperate fully with Entity's breach investigation, response, and any notifications required under applicable federal and state law; and (c) preserve, and not alter or destroy, any records, systems, or evidence related to the incident without Entity's prior written consent.

8. Subcontractors. Contractor shall not share personal data with any subcontractor without prior written approval of Entity, and shall impose data protection obligations at least as protective as those in this addendum on any approved subcontractor before any personal data is shared. Contractor remains fully liable to Entity for the acts and omissions of its subcontractors with respect to personal data.

9. Audit Rights. Entity or its authorized representative may, upon reasonable written notice of not less than ten (10) business days, inspect and audit Contractor's records, systems, and practices relating to personal data received under this agreement, solely for purposes of verifying compliance with this addendum. Contractor shall cooperate fully with any such inspection or audit.

10. Governing Law. This addendum shall be governed by and construed in accordance with the laws of the State of Wyoming, without regard to its conflict of law principles. Any dispute arising under this addendum shall be resolved in the Second Judicial Courts of the State of Wyoming.

ENTITY:

Albany County Fire District #1

By: _____

Date: _____

Name / Title: _____

CONTRACTOR:

Contractor Name: _____

By: _____

Date: _____

Name / Title: _____

DRAFT

Appendix B — Personal Data Access / Objection Request Form

Submit to: *District Chair, Albany County Fire District #1, 4837 N. 3rd Street, Laramie, WY 820702, chair@albanycountyfd1.com*

Note: This form is for a personal data request under W.S. § 9-21-202(b) only. It is not a Wyoming Public Records Act request form.

Requestor to Complete

Request Type (Copy of My Personal Data / Objection to Personal Data): _____

Full Legal Name: _____

Current Address: _____

Wyoming Residency (Current / Former): _____

If Filing on Behalf of Another — Relationship (attach proof of legal authority): _____

Description of Data / Objection: (describe the personal data category, program, date range, or nature of objection)

_____

_____

Objection Basis, if applicable (Accuracy / Completeness / Retention / Dissemination / Denial of Access / Other): _____

Preferred Contact Method (Mail / Email / Phone) and Detail: _____

Requestor Signature and Date: _____

For Official Use Only

Date Received: _____

Received By (Name / Title): _____

Tracking Number: _____

Request Type: ☐ Personal Data Access Request under W.S. § 9-21-202(b) (Statement 7.1 — no statutory deadline; apply the District's published response timeframe) ☐ W.S. § 9-21-201 through § 9-21-203 Written Objection (Statement 7.5 — the District must respond within 60 calendar days of receipt)

Response Due Date: _____

Date of Written Response: _____

DRAFT

Outcome: ☐ Granted ☐ Partially Granted ☐ Denied (state basis) ☐ Meritorious Objection ☐ Lacks Merit ☐ View Statement Added ☐ Wyoming Public Records Act Mandatory Exemption Applied (cite W.S. § 16-4-203 subsection)

Identity Verification — Method Used: _____

Documents Reviewed: _____

Verified By (Name / Title): _____

DRAFT

Appendix C — System Limitation Documentation Form

Complete one form per affected system or technology limitation. File with the District Chair. Retain on file and review annually. See Section 4, Statement 4.7.

Date Completed: _____

Department / Program: _____

System or Technology Affected: _____

Policy Section(s) Affected (e.g., Statement 5.2, Statement 8.2): _____

Description of Limitation: (specifically, what cannot be done and why — be precise; vague acknowledgment does not qualify)

_____

How the Limitation Affects Compliance:

_____

Compensating Controls Implemented:

_____

Remediation Path / Plan (include timeline or budget request reference if applicable):

_____

Estimated Date of Full Compliance ("Unknown — subject to future budget appropriation" is acceptable): _____

Completed By (Name / Title): _____

Submitted To District Chair (Date): _____

Date Acknowledged by District Chair: _____

Next Annual Review Date: _____

DRAFT