(Name of local or special service district)

CRITICAL INFRASTRUCTURE RECORDS POLICY[1]

A. Purpose: This Policy shall be known as the _____ (insert the district's name) ("District") Critical Infrastructure Records Policy or the "Policy", the purpose of which is to protect water and/or wastewater Critical Infrastructure information and records from disclosure and to ensure that any release of said information and records is limited to project-specific data necessitated by a defined development need or governmental purpose.

B. Background:

1. Federal Law: The United States Congress adopted the America's Water Infrastructure Act of 2018 ("AWIA") (Pub. L. No. 115-270), which requires community drinking water systems to conduct a risk and resilience assessment ("RRA") and prepare or revise an emergency response plan ("ERP"). A drinking water system must certify to the U.S. Environmental Protection Agency ("EPA") that the RRA and ERP have been completed every five years. The AWIA protects any information submitted to the EPA from public disclosure (Pub. L. No. 115-270, § 2013(b)). The drinking water system is only required to submit the certification to the EPA, and not the actual RRA and ERP, and thus the public disclosure of the RRA and ERP is subject to state law.

2. State Law: The Government Records Access and Management Act provides that the District's records regarding security measures designed for the protection of persons or property, including building and public works designs relating to ongoing security measures, are not subject to public disclosure (Utah Code Ann. (UCA) § 63G-2-106); protects records if disclosure "would jeopardize the security of governmental property, governmental programs, or governmental recordkeeping systems from damage, theft or other appropriation or use contrary to law or public policy" (UCA § 63G-2-305(12)); and protects the following drinking water and wastewater system records: "(a) an engineering or architectural drawing of the drinking water or wastewater facility; and (b) except as provided in Section 63G-2-106, a record detailing tools or processes the drinking water or wastewater facility uses to secure, or prohibit access to, the records described in Subsection (84)(a)" (UCA § 63G-2-305(84)). In 2022, the Utah Legislature adopted S.B. 254, Government Records Access Revisions, which protects from disclosure certain water and wastewater critical infrastructure records.

3. District Finding: To clarify what District records are protected under GRAMA Section 63G-2-305(12) and (84), the District finds, and for purposes of this Critical Infrastructure Records Policy defines, the following records to be "protected": All engineering and architectural drawings of the District's entire system(s) (including collection, treatment and distribution facilities, as applicable), and all supporting and related documentation such as studies, diagrams, maps, construction renderings, GIS data, work orders, and similar materials, whether in paper, electronic or other format.

C. Definitions: For purposes of this Critical Infrastructure Records Policy the following words will have the following meanings:

[1] This Policy is designed for local districts and special service districts that provide water services, wastewater services, or a combination of water and wastewater services. It is not intended for use by a district that provides neither of those services.

1. "Critical Infrastructure" has the same meaning as in Section 1016(e) of the Patriot Act of 2001 (42 U.S.C. § 5195c(e)): "systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters". Pursuant to Presidential Directive 21, water and wastewater systems are defined as "Critical Infrastructure".

2. "Drinking water facilities" "water facilities" or "wastewater facilities" means the entirety of the District's collection, treatment and distribution system(s), as applicable.

3. "Government Records Access and Management Act" or "GRAMA" means Utah Code Ann. Title 63G, Chapter 2.

4. "Protected" or "Protected Record" has the meaning set forth in Utah Code Ann. § 63G-2-103(20): "a record that is classified [as] protected as provided by Section 63G-2-305."

D. Exempt Records: Pursuant to Section 63G-2-106 of GRAMA, the following records are exempt from and are not subject to the disclosure requirements set forth in GRAMA, and it is the policy of the District that these records shall not be disclosed pursuant to any GRAMA request or other type of records request, except to the extent otherwise required by state or federal law:

1. Security measures and plans, including a plan to prepare for or mitigate terrorist activity, or for emergency and disaster response and recovery. This shall include, but is not limited to, the District's RRA and ERP, as applicable, prepared pursuant to the AWIA. The District's RRA and/or ERP shall include any and all GIS data of the District's Critical Infrastructure systems.

2. Risk Assessment or Security Audit results, or data collected from any risk assessment or security audit performed by the District. This collected data includes any and all GIS data of the District's Critical Infrastructure systems.

3. System and facility data that may disclose points of access to, or vulnerabilities of, the District's collection, treatment and distribution systems, including any and all GIS data, as applicable.

E. Protected Records: Pursuant to Section 63G-2-305(84) of GRAMA, the following records are Protected and are subject to disclosure only to the extent authorized in GRAMA:

1. Records, the disclosure of which would jeopardize the security of governmental property, programs or recordkeeping systems from damage, theft or other appropriation or use contrary to law or public policy. Said records, if not exempt under Subsection D of this Critical Infrastructure Records Policy, include system and facility data that may disclose points of access to, or vulnerabilities of, the District's wastewater collection and treatment and culinary water distribution systems, including GIS data, as applicable.

2. Engineering or architectural drawings of the District's drinking water and/or wastewater facilities, as applicable.

3. Records detailing tools or processes the District uses to secure, or prohibit access to, the records described in Sections B.2 and D.2 of this Policy, except to the extent those records fall within the categories of records described as exempt from disclosure under Section D of this Policy.

F. Public Records: Pursuant to Section 63G-2-106(3) of GRAMA, any certification that the District has conducted a risk and resilience assessment under 42 U.S.C. Sec. 300i-2 is a public record. However, the resulting RRA or ERP, including any supporting data, drawings, summaries, GIS data or information, and other related material, shall not be considered a public record and shall be exempt from disclosure under GRAMA.

G. Policy of Strict Application: It is the intent of the District that this Critical Infrastructure Records Policy be applied strictly to prohibit disclosure of Critical Infrastructure Records and data to the greatest extent allowed under the law and this Critical Infrastructure Records Policy. Due to the security sensitive nature of the District's Critical Infrastructure, any balancing tests set forth in the law shall be weighed more heavily in favor of privacy protection and non-disclosure rather than disclosure. To the extent that the District's Critical Infrastructure GIS data is included within the District's RRA, ERP or any other risk assessment or security audit described in this Critical Infrastructure Records Policy, the District's intent and policy is to keep dissemination of such GIS and related data as restricted as allowed under the law. In its consideration of records requests for the material described herein as exempt or protected, before releasing any such record the District shall require that a requester demonstrate a project specific or other legally justified need for the record. By way of example, the District will release limited project-specific records and data only to owners or developers of property to be served by District facilities, to Blue Stakes utilities and agencies, or to government agencies that have a lawful need for the requested data.

H. Subsequent Modifications/Higher Law:

1. Critical Infrastructure Records Policy Not Exhaustive: The governing body of the District reserves the right to add to, delete from, or change this Critical Infrastructure Records Policy at any time. Each GRAMA request or other request for a record shall be considered on a case-by-case basis, taking into consideration this Critical Infrastructure Records Policy, as well as state and federal laws.

2. Higher Law to Control: In the event of any conflict between the Critical Infrastructure Records Policy and any applicable federal or state law, rule, or regulation, the federal or state law, rule, or regulation, including amendments and modifications thereto, shall control to the extent of such inconsistency.

Approved by the governing body of the District on the ___ day of _____, 20__.

_____

Title: _____