STANDARD OPERATING PROCEDURE FOR DATA HANDLING OF WATER LOCATIONAL DATA AND SERVICE AREA MAPS COLLECTED PURSUANT TO A.R.S. § § 45- 498, 45-454(C) and 45-342(H)(2)

The Arizona Department of Water Resources (ADWR) maintains location data sets for water distribution lines in various Agency databases.

A.R.S. § 45-498 states each city, town, private water company and irrigation district in an active management area shall maintain a current map clearly delineating its service area and distribution system in the director's office and shall furnish such other related data as the director may require and all maps required by this section shall be available for examination by the public at reasonable times.

A.R.S. § 45-454(C) states on or after January 1, 2006, an exempt well may not be drilled on land if any part of the land is within one hundred feet of the operating water distribution system of a municipal provider with an assured water supply designation within the boundaries of an active management area established on or before July 1, 1994, as shown on a digitized service area map provided to the director by the municipal provider and updated by the municipal provider as specified by the director.

A.R.S. § 45-342(H)(2) requires all community water systems in the state to submit to ADWR a description of their existing transmission and distribution facilities and requires all large community water systems to submit a map of those facilities.

ADWR recognizes that the water sector has been identified as one of 11 critical infrastructures by the United States President. As such, the handling and release of location data for critical infrastructure housed in ADWR that could be used for targeting intentional acts of vandalism and terrorism must be uniform and adequately controlled across the Agency.

Water sector critical infrastructure is defined as:

1. Drinking water system wells and surface water intakes
2. Reservoirs
3. Dams
4. Aquifers
5. Drinking water and wastewater treatment facilities
6. Pumping stations
7. Aqueducts
8. Transmission pipelines

ACCESS AND DATA HANDLING BY INDIVIDUALS AUTHORIZED BY ADWR

Only authorized employees of ADWR are allowed to access and receive raw water sector critical infrastructure location data. Authorized secondary users, which include members of the public, may view GIS covers of water sector critical infrastructure data. The authorization and use of water sector critical infrastructure data carries with it the responsibility to adhere to the following specific procedures for handling this sensitive data.

1. **Raw Data Tables:** Direct access to the raw water sector critical infrastructure location data is restricted to authorized employees within ADWR's Water Management Division. No unauthorized person is to have access to the raw data.
2. **Raw Data:** Authorized employees are to store downloaded raw data on ADWR issued computers only. Raw data is not to be stored on removable media such as flash drives and CDs.
3. **GIS Application Using Raw Data Tables:** Only authorized employees are permitted to create geospatial representations with the raw data.
4. **Secondary Users of GIS Application:** Secondary users include members of the public. Authorized employees can create GIS covers for use by secondary users. Secondary users are limited to viewing GIS covers only at the ADWR Office and are not allowed to make copies. Secondary users are required to receive authorization from ADWR's Water Management Division prior to viewing any GIS covers created by authorized employees.
5. **Authorization for Secondary User to View GIS Cover of Water Sector Critical Infrastructure Location Data:** A secondary user may request authorization to view a GIS cover of water sector critical infrastructure location data by completing the attached form and returning it to ADWR's Water Management Division. A person making such a request must provide a description of the need for the data.

REQUEST FOR AUTHORIZATION TO VIEW WATER SECTOR CRITICAL INFRASTRUCTURE DATA

Water Sector Critical Infrastructure raw data is considered SENSITIVE. Care must be taken to ensure this raw data is viewed only by authorized secondary users.

Name:	
Company/Organization: Address: Phone: E-mail:	
Intended Use of Data:	
Signature:	Date: