INDIAN MOUNTAIN METROPOLITAN DISTRICT
DATA PRIVACY POLICY

The District is commtted to protecting the personal privacy of the community and takes seriously its obligation to protect the privacy of data collected, used, shared and stored. Personally Identifiable Information (PII) includes, but is not limited to, information that is collected, maintained, generated, or inferred and that, alone or in combination, personally identifies an individual.

PII, as defined by federal law, also includes other information that, alone or in combination, is linked or linkable to a specific indivifual that would allow a reasonable person in the community, who does not have personal knowledge of the relevant circumstances, to identify the individual with reasonable certainty. As such, to comply with Colorado HB 18-1128, the District has developed and maintains this written policy for the destruction and proper disposal of any document that contains PII; Personal information is not collected through the District's website (www.indianmountain.info).

The District generally only collects personally-identifying information including but not limited to name, postal address, telephone number and email addreses. PII is solely used for communication purposes such as distribution of the community newsletter, notifying a property owner of an issue or concern, or providing IMWSP water augmentation services. The District does not disclose or use the information for any other purposes and PII is maintained on a secured server and/or encrypted devices; files that contain PII are encrypted whenever transmitted electronically. The District disposes of data that is no longer required using secured document destruction methods; electronic records are permantly deleted from devices and files and hard copy records are shredded.

In the unlikely event of a security breach (any incident that results in unauthorized access of data, either physically or electronically including the data's applications, services, networks and/or devices), the District will prompt an investigation and provide notice to any individuals who possibly could be affected by the breach;

- Written notice, to the postal address listed in the records of the individual;
- Telephone notice; or
- Electronic notice, if the primary means of communication with the resident is by electronic means.

Notice will be made in the most expedient time possible and without unreasonable delay, but no later than 30 days after the discovery date of the security breach.