

Public Information Requests for Email & Digital Records

White Paper

Triton Consulting Group, Inc.
July 2nd, 2024

www.tritoncg.com



Google Cloud
Partner

I. Objective

In the public sector space—specifically special purpose districts in the State of Texas— we have observed a steady and consistent shift toward digital technologies and solutions. The purpose of technology is to either perform a task, solve a problem, or make the action of these simpler/faster—but that only works when they are implemented correctly.

As technology continues to become the standard, it behooves the industry to ensure that any digital transformation is prepared to manage requests that come through the Freedom of Information Act (FOIA) and Public Information Requests (PIRs).

The following recommendations are compiled based on our technological insight, historical experience, and the strategies that have allowed public organizations to respond accurately and promptly to such requests.

II. Background

Triton Consulting Group, Inc. has worked closely with Special Purpose Districts in the State of Texas for over 20 years providing consulting services ranging from public relations, internal communications process adoption, and technology administration. In 2024, Triton began a strategic partnership with Google Public Sector to further develop Google’s cloud products with an emphasis on public sector integration.

III. Example Case

One of our clients, received a Public Information Request (PIR) under the Freedom of Information Act (FOIA). The request contained many items, broadly naming semi-specific communication records including emails and messages, within a 4 year time period. Given the volume and sensitivity of the information, the organization required a comprehensive and efficient methodology by which to clearly define, locate, preserve, and produce the requested data. Fortunately, we had previously implemented well-defined architecture, policies, and procedures to enable fast and complete fulfillment of public information requests within the legally required response time—regardless of the requests voluminous nature.

IV. Policies & Practices

The following policies and practices have proven essential components in accomplishing the defined Objective.

A. Foresight

Premeditation is the first, and arguably the most crucial, component required to ensure both the preservation and integrity of digital data when satisfying PIRs. The architecture

and policies to meet these needs must be defined before records are requested. Neglecting this step will invariably result in unreasonable difficulty and/or impossibility when attempting to respond to PIRs.

B. Establishing an Intelligent Communication Policy

1. Adopt a Communication Policy to standardize practices, mitigate potential violations, and improve compliance.
2. Establish policy mandating domain(s), email accounts, and devices be centrally managed.
3. Establish a retention policy to support compliance with Public Information Act/FOIA requests.
4. Establish policy prohibiting use of personal devices and/or email accounts to limit exposure across devices and platforms.

C. Assign Agency/Stewardship for Digital Data Retention

1. Ensure all digital data is managed in accordance with District policies by an assigned party/administrator/consultant.
2. Contract professionals familiar with your entity's anatomy, public sector requirements. Vet your candidates fully prior to engagement, using your legal counsel, if available.

V. Tactical PIR Process:

All PIRs will follow the same five basic steps: Receipt, and Validation, Interpretation, Translation to Query, Production of Results, Preparation and Delivery. We outline each below.

A. Receipt and Validation

Often, these requests may be received with improper phraseology thereby nullifying the request and requiring General Counsel to, in essence, "decline" the request. The first step, therefore, is to acknowledge receipt and verify that it is a valid request.

B. Interpretation

As most PIRs do not originate from those well-versed in the rules and procedures for these requests, they often contain unclear, overreaching, overly-broad, or otherwise ambiguous requests that require translation and interpretation from general counsel.

Only once they have been interpreted and/or clarified can the newly refined request can be processed.

I.e. - A request may read "All email messages to boardmemberx@domain.com in 2023."

General Counsel will typically note the original request language does not include:

1. Specified time zone for the date range
2. Request for email attachments
3. Request for emails *from* boardmemberx@domain.com

General Counsel would typically provide clarification on the details of these specificities as part of the Interpretation phase prior to sending the request on.

C. Translation to Query

The current interpreted request then must be translated to specific queries. As digital systems do not allow for any analog ambiguity, queries must be phrased exactly.

I.e. - Using the prior request example Translated to a Query, might be formatted as such:

[Type: (Email)]
[Sent: between 2023-01-01 and 2023-12-31]
[Time zone:(America/Chicago)]
[Terms:(to:boardmemberx@domain.com)]
[Accounts:(boardmemberx@domain.com)]

D. Production of Results

Systems with proper eDiscovery tools will enable accurate and fast export of the request into a standardized file format once the query parameters are validated and defined. This Production export is then delivered to General Counsel for review. If General Counsel receives Production files in mixed, uncommon, or unknown formats, this can drastically reduce the efficiency of the final response package. File format and ease-of-access are high priority items to address prior to delivery of Production.

E. Preparation & Delivery

General Counsel must manually review, filter for confidentiality or privilege, and sort the production items for delivery. General Counsel then compiles the results and delivers the final production to the requester.

Given the limited time allowed for response to public information requests, efficiency and advance planning are paramount for legal compliance.

Conclusion

Production of digital public records very closely resembles existing practices for legal Discovery in litigation—but with a much shorter response window as, generally, requests in the State of Texas must be fulfilled within 10 working days from the initial request. With that timeline in mind, failure or improper application of processes can delay the entire production and subject the entity to possible sanction.