From: **Kyle Moring** [redacted]
Subject: GOVERNANCE NOTICE – Confidential SSN Exposure Notice Sent to City Administration/OpenGov Coordination
Date: April 28, 2026 at 8:24 PM
To: Wesley Lyon wlyon@mtpleasanttx.gov, chinton@mtpleasanttx.gov, dcorbell@mtpleasanttx.gov, kredfearn@mtpleasanttx.gov, jhageman@mtpleasanttx.gov, melanie.knight@mtpleasanttx.gov, Carl Hinton chinton@mpcity.org, dcorbell@mpcity.org, kredfearn@mpcity.org, jhageman@mpcity.org, Melanie.knight@mpcity.org
Cc: Rob Vine rvine@mtpleasanttx.gov, Candias Webster cwebster@mtpleasanttx.gov, Lea Ream lream@dtrglaw.com, Austin Beck abeck@dtrglaw.com

Mayor and Council Members:

I am providing this sanitized governance notice so the governing body is aware that I have today sent a confidential security/privacy notice to City administration and counsel concerning an apparent public exposure of Social Security numbers in the City of Mount Pleasant's OpenGov-hosted financial transparency portal.

This is not a Texas Public Information Act request. I am not including any full Social Security numbers, row-level findings, password, attachment, or unredacted evidence in this council notice.

I have intentionally omitted the direct portal URL from this council notice because the apparent exposure may still be active. The direct portal URL and row-level information were provided separately to City administration and counsel for containment, preservation, and remediation review.

Summary

Using ordinary public access only – no authentication, circumvention, exploitation, or nonpublic endpoint access – I reviewed the City's publicly available Accounts Payable transparency dataset export.

The export contains 456,623 records and 102 columns. A pattern-based review identified 21 distinct apparent SSN-format values that pass standard validity-exclusion checks, appearing in 692 findings across 645 unique source dataset rows. Forty-seven source rows contain two distinct apparent SSN findings.

The apparent SSNs appear in vendor/address, vendor-attention, and invoice-related fields. For records with populated check dates, the affected records range from March 7, 1995 through August 27, 2009; one finding row does not have a populated check date.

Some affected records appear to involve employee, former employee, or employee-related payment records. I have not included any individual SSN or row-level information in this council notice.

Reason for this notice

I am sending this to the Council because I have previously raised concerns regarding the City's public information, transparency, and records-handling practices, and this issue now appears to involve potential public exposure of sensitive personal information through the City's public-facing financial transparency system.

My purpose in notifying the Council is governance awareness only. The operational details, encrypted evidence, and follow-up should be handled by City administration, records management, legal counsel, and appropriate technical personnel.

Requested City action

In the confidential notice to City administration and counsel, I requested that the City:

1. Immediately contain the exposure by taking the affected report offline, disabling public export/access, filtering affected records, or otherwise preventing continued public access to the affected records while the City investigates;
2. Preserve the current public-facing report, underlying source records, OpenGov configuration, publication/ingestion history, audit logs, access/export logs, administrative action logs, and remediation records;
3. Coordinate with OpenGov to determine how the affected records were published, whether the exposure remains active, and whether any third-party downloads, exports, or access events are reflected in available logs;
4. Review the affected records to determine the identity, residency status, and living/deceased status of affected individuals, including whether any affected individuals are current or former City employees;
5. Determine whether any individual notice, Attorney General notice, data-security notice, public-information compliance action, or other legal obligation is triggered; and
6. Review the remainder of the City's transparency-publication set for similar personally identifiable information or sensitive personal

information.

OpenGov notice

I am also notifying OpenGov separately as the apparent platform host/operator for the public portal so that OpenGov can assist the City with containment, preserve relevant platform records and logs, and coordinate with the City regarding remediation.

Please do not reply-all with substantive discussion of this matter. To avoid unnecessary dissemination of sensitive information and to preserve appropriate process, I respectfully request that Council members route any follow-up through the City Manager and City Attorney.

Respectfully,

Kyle Moring

[redacted] | [redacted]

From: **Kyle Moring** [redacted]
Subject: Re: GOVERNANCE NOTICE – Confidential SSN Exposure Notice Sent to City Administration/OpenGov Coordination
Date: April 29, 2026 at 10:38 AM
To: Wesley Lyon wlyon@mtpleasanttx.gov, chinton@mtpleasanttx.gov, dcorbell@mtpleasanttx.gov, kredfearn@mtpleasanttx.gov, jhageman@mtpleasanttx.gov, melanie.knight@mtpleasanttx.gov, Carl Hinton chinton@mpcity.org, dcorbell@mpcity.org, kredfearn@mpcity.org, jhageman@mpcity.org, Melanie.knight@mpcity.org
Cc: Rob Vine rvine@mtpleasanttx.gov, Candias Webster cwebster@mtpleasanttx.gov, Lea Ream lream@dtrglaw.com, Austin Beck abeck@dtrglaw.com

Mayor Lyon and Members of the City Council:

I am providing this sanitized governance notice so the governing body is aware that I have sent a supplemental confidential security/privacy notice to City administration and counsel concerning an additional category of apparent confidential information identified in the City of Mount Pleasant's OpenGov-hosted financial transparency dataset.

This is not a Texas Public Information Act request. I am not including any dates of birth, patient case numbers, victim-identifying details, provider names, row-level findings, passwords, attachments, or unredacted evidence in this Council notice.

The detailed evidence has been provided separately to City administration and counsel in encrypted form for containment, preservation, and legal review.

Summary

Yesterday, I notified the City regarding apparent Social Security number exposure in the City's publicly available Accounts Payable transparency dataset. A subsequent review of the same dataset identified a separate and more sensitive category of apparent exposure: records that appear to involve sexual assault forensic medical examination payment records, patient-identifying information, and at least one record that appears to involve a minor patient.

Using ordinary public access only – no authentication, circumvention, exploitation, or nonpublic endpoint access – I reviewed the City's publicly available Accounts Payable transparency dataset. The follow-up review identified:

1. Two records in which an invoice-related field appears to disclose patient-identifying information associated with forensic medical examination records; and
2. A broader set of approximately 45 Accounts Payable records from 2008 through 2015 that appear to correspond to approximately 35 distinct sexual assault forensic medical examination payment records.

At least one identified record appears, from the date-of-birth context, to involve a patient who was approximately 13 years old at the time of the examination.

Access-status update

The records were still publicly accessible through the OpenGov-hosted portal as of approximately 5:11 AM CT on Wednesday, April 29, 2026. When I rechecked at approximately 9:25 AM CT the same morning, the link appeared to no longer function or was no longer accessible from my browser.

I cannot determine from public access alone whether the records were removed, the report was disabled, access was restricted, or another technical change occurred. Because the public-facing state appears to have changed between those two times, I have asked City administration and counsel to preserve records sufficient to determine what changed, who initiated the change, when it occurred, and what data remained accessible before and after the change.

Reason for this notice

I am sending this Council notice for governance awareness only. The operational details, encrypted evidence, and follow-up should be handled by City administration, records management, legal counsel, technical personnel, and OpenGov.

This issue appears to raise confidentiality, privacy, breach notification, records-management, public-information, and financial transparency control concerns. The records appear to involve sensitive victim/patient-identifying information in the City's public financial transparency publication environment.

Requested City action

In the confidential notice to City administration and counsel, I requested that the City:

In the confidential notice to City administration and counsel, I requested that the City:

1. Confirm whether the affected report has been disabled, removed, restricted, filtered, or otherwise remediated, and confirm that continued public access to the apparent victim/patient-identifying information has stopped;
2. Preserve the public-facing report state before and after the apparent access change between approximately 5:11 AM CT and 9:25 AM CT on Wednesday, April 29, 2026;
3. Preserve the underlying Accounts Payable source records, OpenGov configuration, ingestion history, publication history, field-mapping records, administrative action logs, export/access logs, API/request logs if retained, and all remediation records;
4. Coordinate with OpenGov to determine whether the apparent access change resulted from City action, OpenGov action, report disablement, permission change, filter change, deletion, export restriction, or another technical event;
5. Determine whether the affected records were downloaded, exported, accessed, indexed, cached, or otherwise retrieved by third parties during the period of public availability;
6. Review the affected records to determine whether individual notice, breach notice, medical privacy notice, public-information compliance action, or other legal obligation is triggered; and
7. Review the remainder of the City's public financial transparency datasets for similar sensitive personal information before continuing public publication.

OpenGov notice

I am also notifying OpenGov separately as the apparent platform host/operator for the public portal so that OpenGov can assist the City with containment, preserve relevant platform records and logs, identify the access-status change that appears to have occurred this morning, and coordinate with the City regarding remediation.

Please do not reply-all with substantive discussion of this matter. To avoid unnecessary dissemination of sensitive information and to preserve appropriate process, I respectfully request that Council members route any follow-up through the City Manager and City Attorney.

Respectfully,

Kyle Moring

[redacted] | [redacted]

> On Apr 28, 2026, at 8:24 PM, Kyle Moring <[redacted] > wrote:
>
> Mayor and Council Members:
>
> I am providing this sanitized governance notice so the governing body is aware that I have today sent a confidential security/privacy notice to City administration and counsel concerning an apparent public exposure of Social Security numbers in the City of Mount Pleasant's OpenGov-hosted financial transparency portal.
>
> This is not a Texas Public Information Act request. I am not including any full Social Security numbers, row-level findings, password, attachment, or unredacted evidence in this council notice.
>
> I have intentionally omitted the direct portal URL from this council notice because the apparent exposure may still be active. The direct portal URL and row-level information were provided separately to City administration and counsel for containment, preservation, and remediation review.
>
> **Summary**
>
> Using ordinary public access only – no authentication, circumvention, exploitation, or nonpublic endpoint access – I reviewed the City's publicly available Accounts Payable transparency dataset export.
>
> The export contains 456,623 records and 102 columns. A pattern-based review identified 21 distinct apparent SSN-format values that pass standard validity-exclusion checks, appearing in 692 findings across 645 unique source dataset rows. Forty-seven source rows contain two distinct apparent SSN findings.
>
> The apparent SSNs appear in vendor/address, vendor-attention, and invoice-related fields. For records with populated check dates, the affected records range from March 7, 1995 through August 27, 2009; one finding row does not have a populated check date.

Some affected records appear to involve employee, former employee, or employee-related payment records. I have not included any individual SSN or row-level information in this council notice.

Reason for this notice

I am sending this to the Council because I have previously raised concerns regarding the City's public information, transparency, and records-handling practices, and this issue now appears to involve potential public exposure of sensitive personal information through the City's public-facing financial transparency system.

My purpose in notifying the Council is governance awareness only. The operational details, encrypted evidence, and follow-up should be handled by City administration, records management, legal counsel, and appropriate technical personnel.

Requested City action

In the confidential notice to City administration and counsel, I requested that the City:

1. Immediately contain the exposure by taking the affected report offline, disabling public export/access, filtering affected records, or otherwise preventing continued public access to the affected records while the City investigates;
2. Preserve the current public-facing report, underlying source records, OpenGov configuration, publication/ingestion history, audit logs, access/export logs, administrative action logs, and remediation records;
3. Coordinate with OpenGov to determine how the affected records were published, whether the exposure remains active, and whether any third-party downloads, exports, or access events are reflected in available logs;
4. Review the affected records to determine the identity, residency status, and living/deceased status of affected individuals, including whether any affected individuals are current or former City employees;
5. Determine whether any individual notice, Attorney General notice, data-security notice, public-information compliance action, or other legal obligation is triggered; and
6. Review the remainder of the City's transparency-publication set for similar personally identifiable information or sensitive personal information.

OpenGov notice

I am also notifying OpenGov separately as the apparent platform host/operator for the public portal so that OpenGov can assist the City with containment, preserve relevant platform records and logs, and coordinate with the City regarding remediation.

Please do not reply-all with substantive discussion of this matter. To avoid unnecessary dissemination of sensitive information and to preserve appropriate process, I respectfully request that Council members route any follow-up through the City Manager and City Attorney.

Respectfully,

Kyle Moring

[redacted] | [redacted]