Transforming How Texas Government Serves Texans

Local Government Incident Reporting

User Guide

Version 1.1

March 1, 2024

Table of Contents

Overview

Texas Government Code 2054.603 requires state agencies and local governments that experience a security incident to:

1. report to DIR within 48 hours after discovery (or notify the secretary of state if the incident involves election data), and
2. comply with the notification requirements of Section 521.053, Business & Commerce Code, to the same extent as a person who conducts business in this state.

State agencies and local governments must report to DIR the details of the security incident and an analysis of the cause of the incident within 10 days after incident eradication, closure, and recovery.

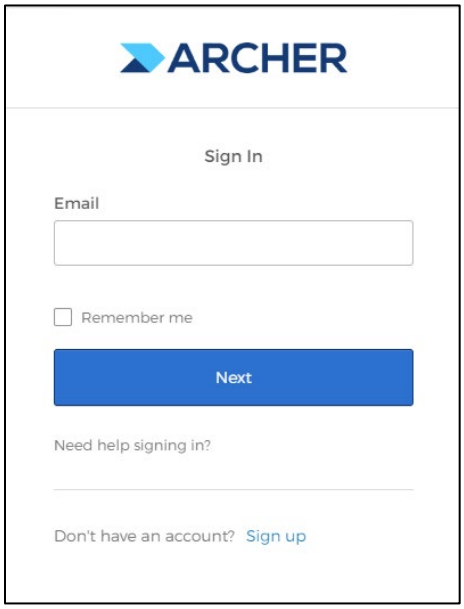
Local governments submit incidents to DIR using Archer Engage, https://engage.archerirm.us/new/32ec31b7-cb95-4c18-9594-bfdb3ea776f9.

Logging In

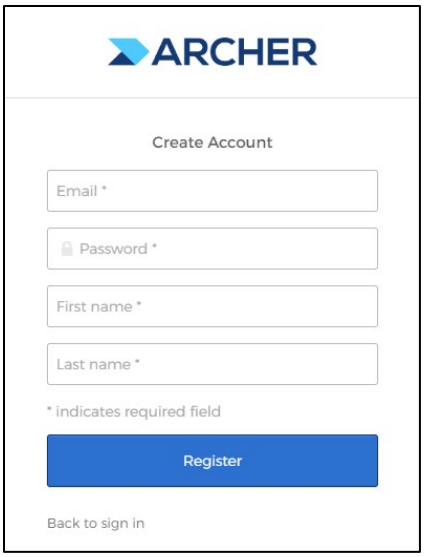
To log into the incident reporting system, you can navigate to the Local Incident Reporting System, which can also be accessed through DIR's website.

First-Time Users

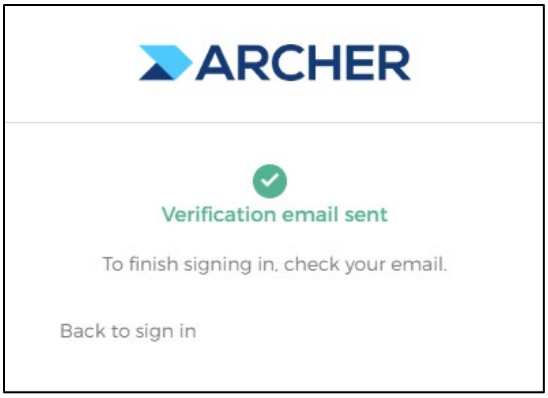
1. If this is your first time logging in to submit an incident, start by going to the Local Incident Reporting System and choosing **Sign up**.



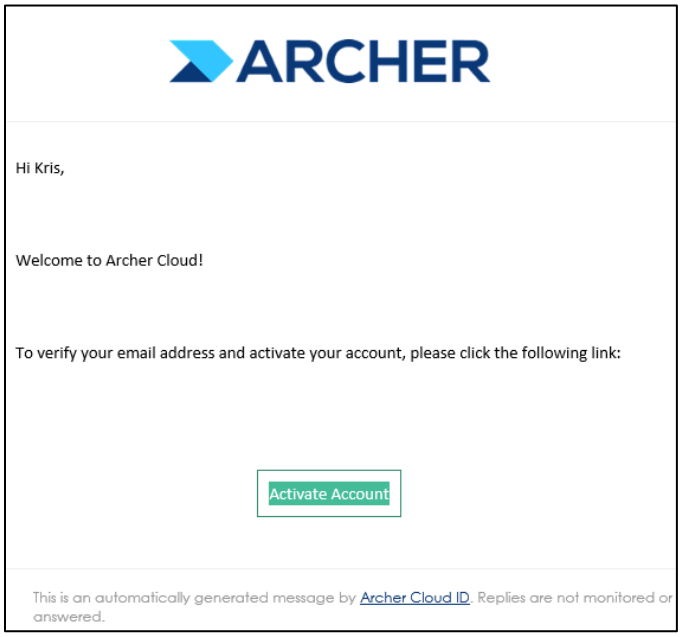
2. Enter your information in the fields (note that every field is required) and click **Register**.



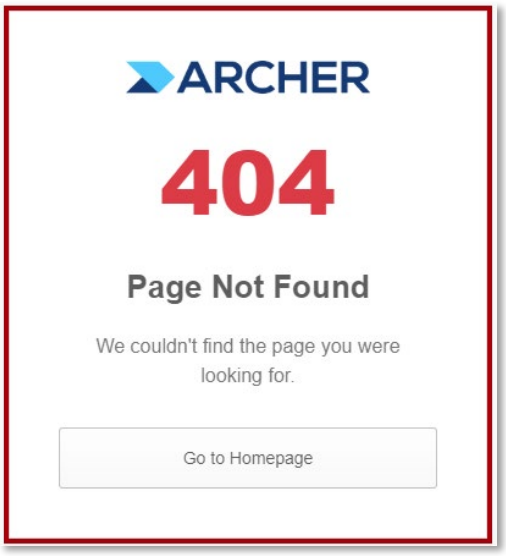
3. You will see a pop-up that a verification has been sent to your email.



4. You will receive an email from <Archer Cloud ArcherCloudID@archerirm.com>.

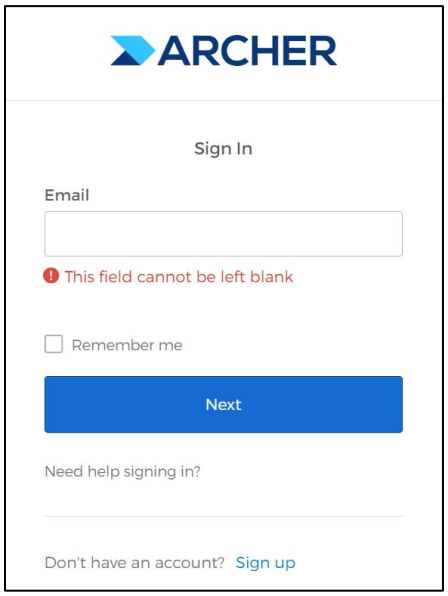


5. Click **Activate Account**.
6. If you get the error below, navigate back to the Local Incident Reporting System, and you should be able to log in and submit an incident report.

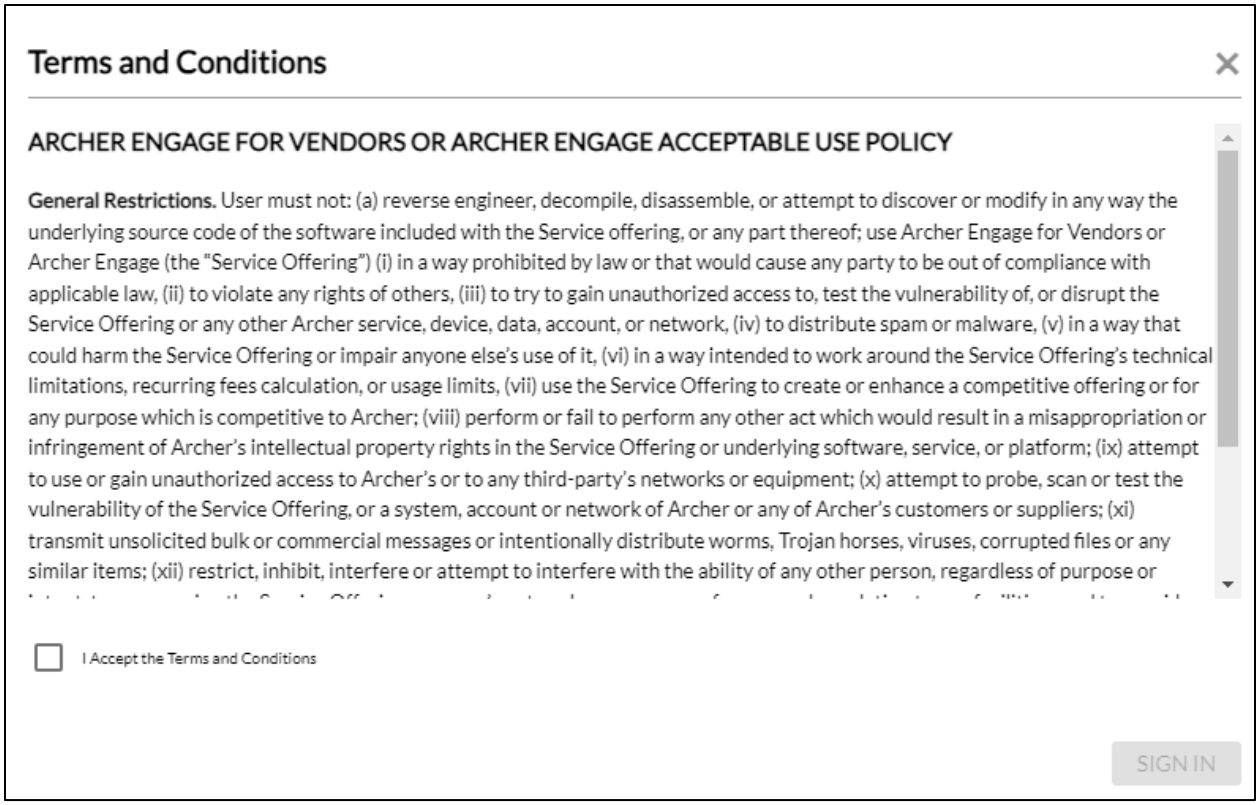


Logging In (After Creating an Account)

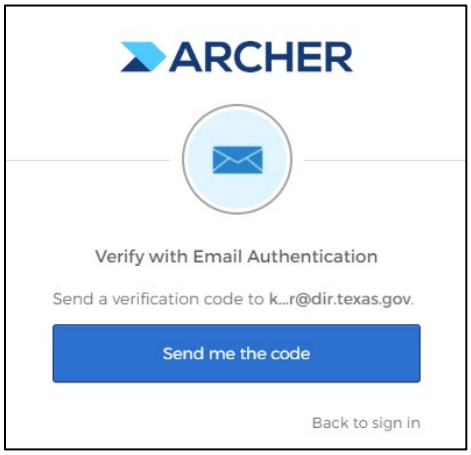
1. Navigate to the incident report URL, https://engage.archerirm.us/new/32ec31b7-cb95-4c18-9594-bfdb3ea776f9, or to the closure/post-mortem report URL (from the incident confirmation email).



2. Enter your email and click **Next**.
3. Enter your password and click **Sign In**.
4. Accept the Terms and Conditions. (You will only have to do this the first time you log in.) Review the terms and conditions and then click the box in the lower left corner to Accept.

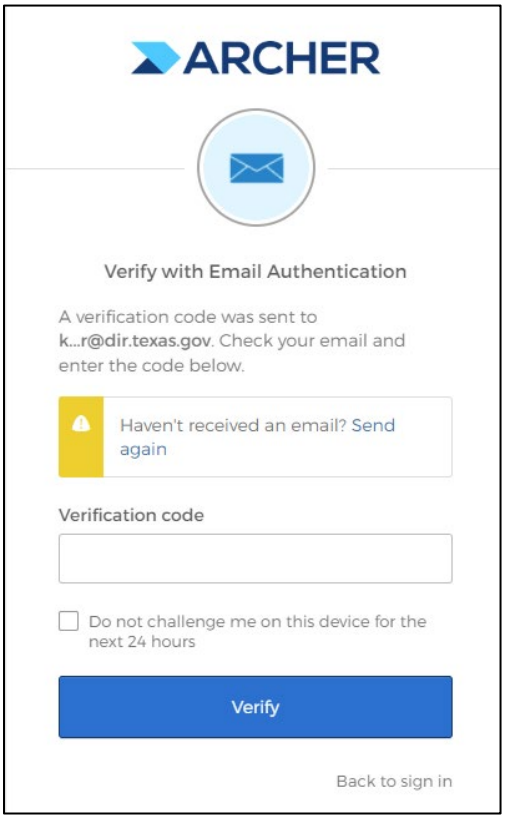


5. You will then be sent a verification code to your email that you will use to complete the login process. Click **Send me the code** to continue.

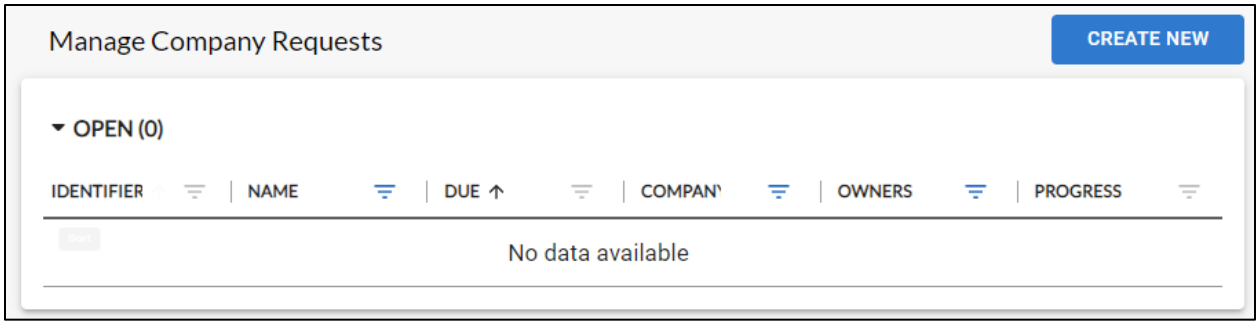


6. The email will look like this.

7. You will then see the following screen prompting you to enter the code that you received via email. You may see a pop-up that asks if you haven't received an email. Click **Send again** if you didn't receive an email. After you receive your code, enter it in the Verification code box and click **Verify**.



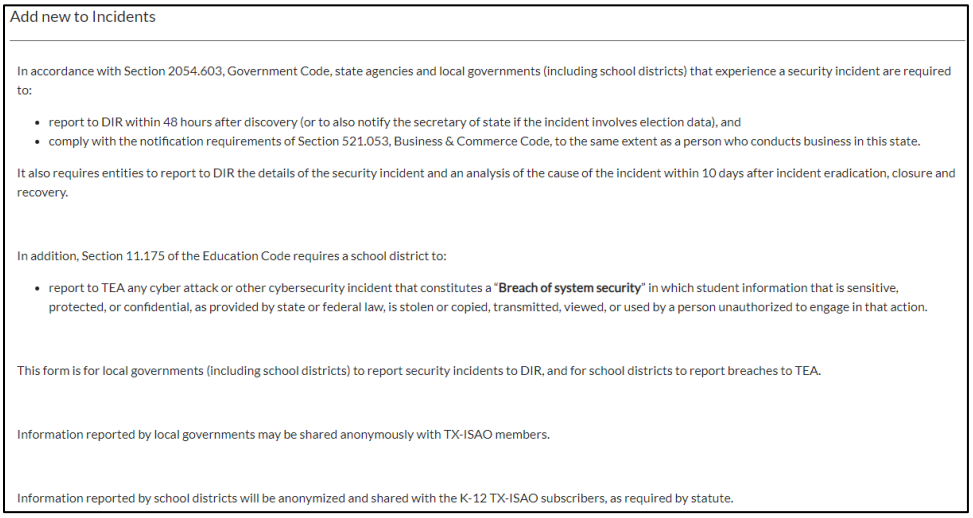
8. After logging in, your screen may look like the one below. Navigate to the incident or closure/post-mortem URL again to be directed to the applicable form.



Incident Report

Submitting an Incident Report

1. Navigate to the incident URL, https://engage.archerirm.us/new/32ec31b7-cb95-4c18-9594-bfdb3ea776f9, and you will see this screen:

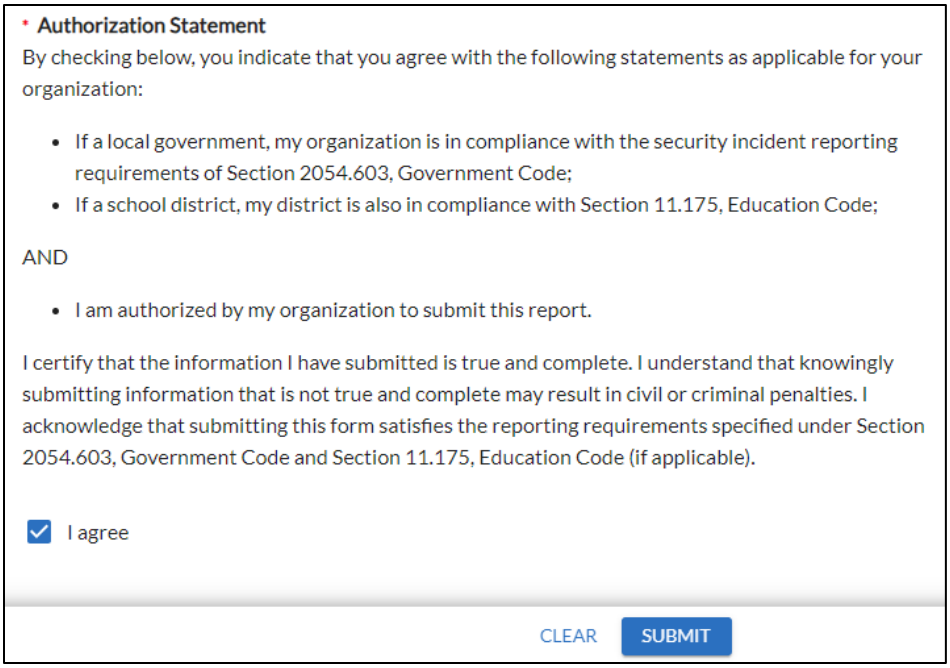


2. Complete the incident report. The following fields are required to submit your incident:
   a. Are you submitting an incident on behalf of another organization? (If yes, provide submitter's organization name, first name, last name, email address, and phone number.)
   b. Affected Organization Point of Contact: First Name, Last Name, Email Address, Title, Phone Number
   c. Incident Name
   d. Agency Type: School District or Local Government
   e. Agency Name
   f. Local Incident Discovery Date
   g. (For School Districts) Does this incident meet the definition of Texas Education Code 11.175 for a breach of system security? (If yes, TEA will be notified and information reported will be anonymized and shared with the K-12 TX-ISAO subscribers, as required by statute.)
   h. Local Incident Type:
      - Basic Web Attacks
      - Compromised Account

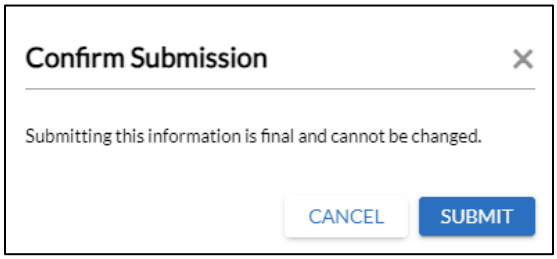
- Data Breach
- Defacement
- Denial of Service
- Lost/Stolen Device
- Inadvertent Disclosure
- Malware (General)
- Phishing
- Ransomware
- Other (please specify)

i. Have any indicators of compromise been identified that can be shared? (If yes, provide IOCs.)
j. Was non-public data disclosed?
k. Was this incident reported to law enforcement? (If yes, provide agency name)
l. Can this incident propagate to other systems?
m. Incident Summary
n. Would you like a consultation with DIR's Cybersecurity Incident Response Team? (If yes, a member of the CIRT will contact you to review previous actions, current priorities, and next steps, and may provide guidance and recommendations as appropriate.)
o. Certification checkbox

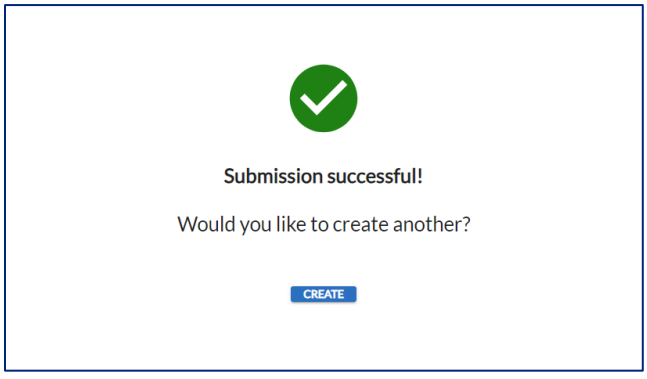
3. The following fields are not required but are encouraged:
   a. Priority
      - Critical: The incident should be dealt with immediately
      - High: The incident should be dealt with within two business days
      - Medium: The incident should be dealt with within five business days
      - Low: The incident should be dealt with within ten business days
   b. Containment Date
   c. Can this incident be classified as ransomware?
   d. How many records were compromised?
4. Before submitting, you will be required to sign a certification statement.



5. Once all required fields are completed, the Submit button will be enabled. Click **Submit** and you will see a pop-up confirming your submission. Click **Submit** again to finalize your submission.



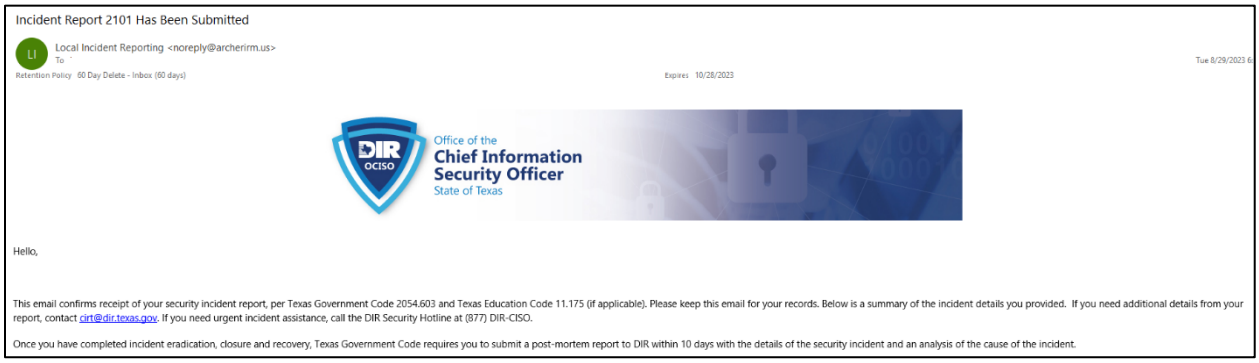
6. It may take a few moments to submit. Please be patient and refrain from taking any action until you see the following screen, which confirms the incident has been submitted.



7. After submitting your incident, if you need urgent incident assistance, please call (877) DIR-CISO or (877) 347-2476.

Incident Confirmation Email

1. Within 30 minutes, you will receive a confirmation email from Local Incident Reporting noreply@archerirm.us with the subject line **Incident Report XXXXX Has Been Submitted**. (If the incident was submitted by a 3rd party, the 3rd party submitter and the organization's point of contact will each receive a confirmation email.)


Incident Report 2101 Has Been Submitted

Local Incident Reporting <noreply@archerirm.us>
To

Retention Policy 60 Day Delete - Inbox (60 days) Expires 10/28/2023 Tue 8/29/2023 6

Office of the Chief Information Security Officer State of Texas

Hello,

This email confirms receipt of your security incident report, per Texas Government Code 2054.603 and Texas Education Code 11.175 (if applicable). Please keep this email for your records. Below is a summary of the incident details you provided. If you need additional details from your report, contact cirt@dir.texas.gov. If you need urgent incident assistance, call the DIR Security Hotline at (877) DIR-CISO.

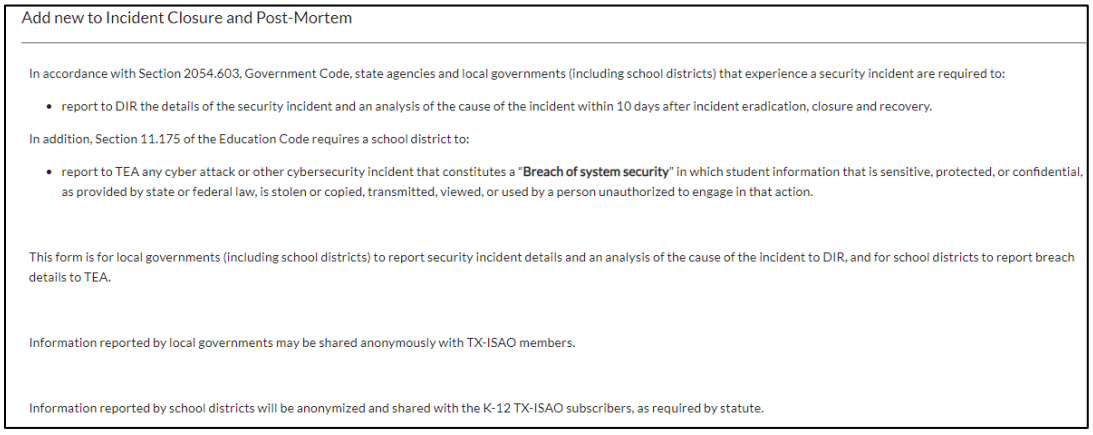
Once you have completed incident eradication, closure and recovery, Texas Government Code requires you to submit a post-mortem report to DIR within 10 days with the details of the security incident and an analysis of the cause of the incident.

2. The email will contain some of the fields submitted on the incident report. If you need additional details from your report, contact CIRT@dir.texas.gov.
3. The email will include a link to the closure/post-mortem report which must be submitted by the affected organization within 10 days of incident eradication, closure, and recovery.
4. Retain this confirmation email as it includes information that will be needed to submit the closure/post-mortem report.

Closure/Post-Mortem Report

Submitting a Closure/Post-Mortem Report

1. Navigate to the closure/post-mortem URL (for this link, please refer to the incident confirmation email).
2. If needed, log into Archer Engage. If after logging in, you are not redirected to the closure/post-mortem form, navigate to the closure/post-mortem URL again.


Add new to Incident Closure and Post-Mortem

In accordance with Section 2054.603, Government Code, state agencies and local governments (including school districts) that experience a security incident are required to:

- report to DIR the details of the security incident and an analysis of the cause of the incident within 10 days after incident eradication, closure and recovery.

In addition, Section 11.175 of the Education Code requires a school district to:

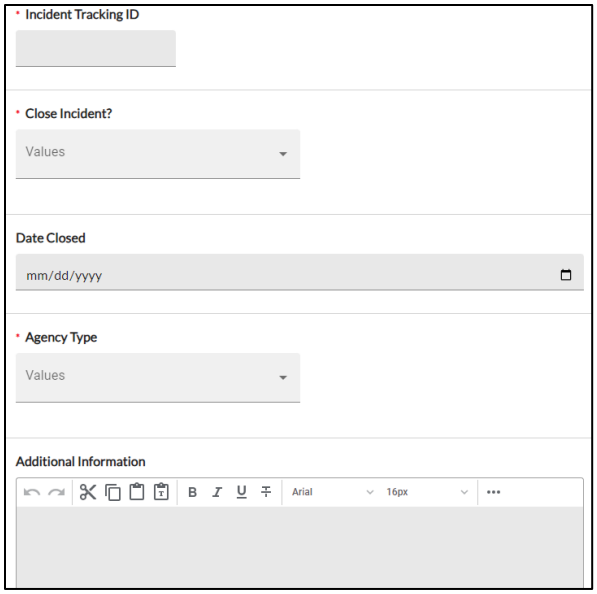
- report to TEA any cyber attack or other cybersecurity incident that constitutes a "**Breach of system security**" in which student information that is sensitive, protected, or confidential, as provided by state or federal law, is stolen or copied, transmitted, viewed, or used by a person unauthorized to engage in that action.

This form is for local governments (including school districts) to report security incident details and an analysis of the cause of the incident to DIR, and for school districts to report breach details to TEA.

Information reported by local governments may be shared anonymously with TX-ISAO members.

Information reported by school districts will be anonymized and shared with the K-12 TX-ISAO subscribers, as required by statute.

3. Make sure you have your Incident ID from the incident confirmation email. You will need to enter it into the closure/post-mortem report.



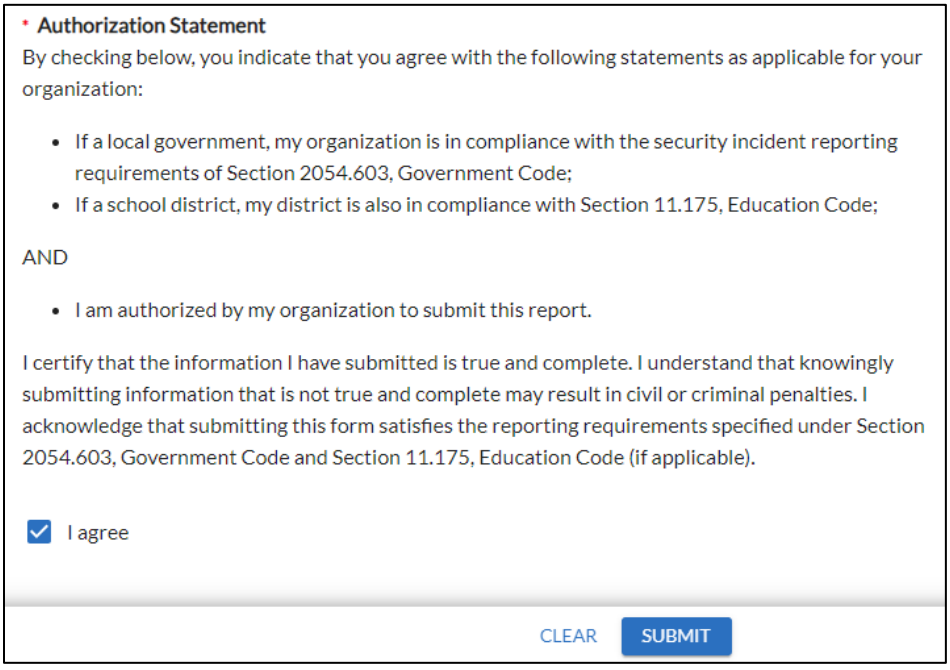
4. Complete the closure/post-mortem report. The following fields are required to submit your closure/post-mortem report:
    a. Incident Tracking ID (i.e. Incident ID)
    b. Close Incident (if yes, provide Date Closed)
    c. Agency Type
    d. Agency Name
    e. Does this incident involve a confirmed or suspected breach of system security as defined by Section 521.053, Business & Commerce Code? (If yes, additional fields will be required.)
    f. (For School Districts) Does this meet the definition of Texas Education Code Section 11.175 for a breach of system security? (If yes, additional fields will be required.)
    g. (Optional) Additional Information
5. If the incident involves a confirmed or suspected breach of system security as defined by Section 521.053, Business & Commerce Code, the following fields are required:
    a. Incident Summary
    b. Incident Type
        - Compromised Account
        - Data Breach
        - Defacement
        - Denial of Service
        - Lost/Stolen Device
        - Inadvertent Disclosure
        - Malware (General)
        - Phishing
        - Ransomware
        - Basic Web Attacks
        - Other (please specify)
    c. Have any indicators of compromise been identified that can be shared? (If yes, provide IOCs.)

d. (Optional) Which of the following best describes the overall impact of the incident on the organization?
    - Catastrophic - Irrecoverable effects and permanent critical organizational damage
    - Damaging - Significant long-term effects and/or substantial impact on delivery of critical systems and staff operations
    - Distracting - Limited hard costs, impact felt through reallocation of staff duties
    - Insignificant - Impact absorbed by normal activities
    - Painful - Limited hard costs, significant disruption of business services and/or normal staff operations
    - Unknown
e. Please provide an analysis of the cause of the incident.
f. (Optional) What corrective action(s) are planned (or recommended) to prevent and/or detect similar incidents in the future? This can include general recommendations, specific changes to policy, procedures, personnel, and technology, short-term and long-term strategies, etc.

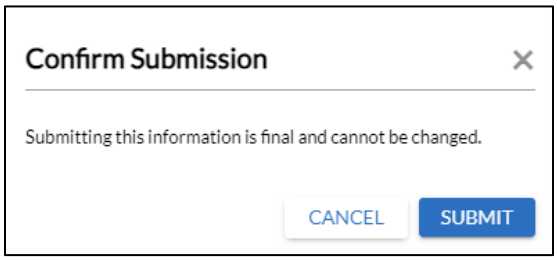
6. (For School Districts) If the incident meets the definition of Texas Education Code Section 11.175 for a breach of system security, the following fields are required:
    a. Incident Summary
    b. Incident Type
        - Data Breach
        - Defacement
        - Denial of Service
        - Lost/Stolen Device
        - Inadvertent Disclosure
        - Malware (General)
        - Phishing
        - Ransomware
        - Basic Web Attacks
        - Other (please specify)
    c. Have any indicators of compromise (IOCs) been identified that can be shared? (If yes, provide IOCs)
    d. Does the breach involve a user device (desktops, laptops, phones, etc.), server(s) or a third party or other?
        - User Device(s)
        - Server(s)
        - Third Party
        - None of the above
        - Other (please specify)
    e. What threat actors were involved?
        - External
        - Internal
        - Vendor/Trusted Third-Party
        - Unknown
    f. Was student personally identifiable information (PII) or sensitive information exposed?

g. (Optional) How many student records were compromised?
h. Has your ESC been notified?
i. What external resources and steps were taken to resolve the incident?
j. Does your organization have cyber insurance? (If yes, did your organization leverage cyber insurance for this incident?)
k. (Optional) If applicable, have there been any mitigating control factors added to prevent similar future incidents? (If yes, explain.)
l. Estimated hours spent to resolve incident.
m. Additional information (TEA reporting requirements affected, etc.)
n. (Optional) Which of the following best describes the overall impact of the incident on the organization?
    - Catastrophic - Irrecoverable effects and permanent critical organizational damage
    - Damaging - Significant long-term effects and/or substantial impact on delivery of critical systems and staff operations
    - Distracting - Limited hard costs, impact felt through reallocation of staff duties
    - Insignificant - Impact absorbed by normal activities
    - Painful - Limited hard costs, significant disruption of business services and/or normal staff operations
    - Unknown
o. Please provide an analysis of the cause of the incident.
p. (Optional) What corrective action(s) are planned (or recommended) to prevent and/or detect similar incidents in the future? This can include general recommendations, specific changes to policy, procedures, personnel, and technology, short-term and long-term strategies, etc.

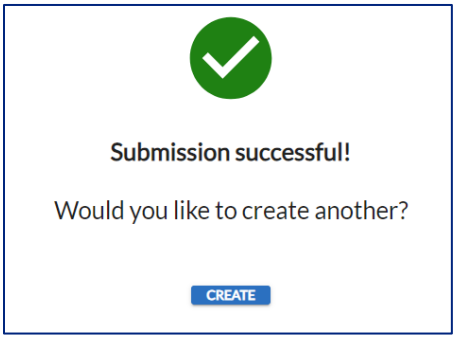
7. Before submitting, you will be required to sign a certification statement.



8. Once all required fields are completed, the Submit button will be enabled. Click **Submit** and you will get a pop-up confirming your submission. Click **Submit** to finalize your submission.

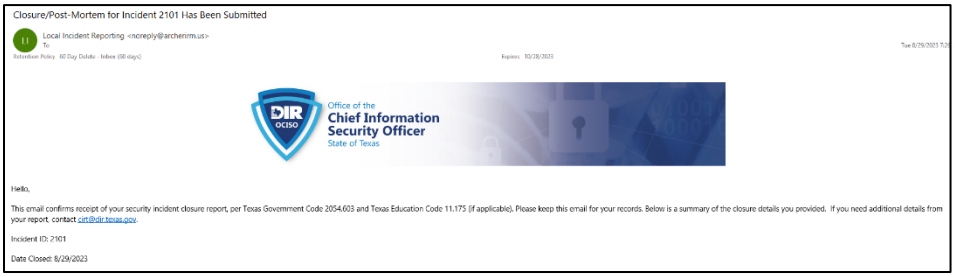


9. It may take a few moments to submit. Please be patient - do not click submit again. When the closure/post-mortem has been submitted, you will see this screen.



Closure/Post-Mortem Confirmation Email

1. Within 35 minutes, you will receive a confirmation email from Local Incident Reporting noreply@archerirm.us with the subject line **Closure/Post-Mortem for Incident XXXXX Has Been Submitted**.



2. The email will contain some of the fields submitted on the closure/post-mortem report. If you need additional details form your report, contact CIRT@dir.texas.gov.

Additional Information

Incident (Alternate Submission Option)

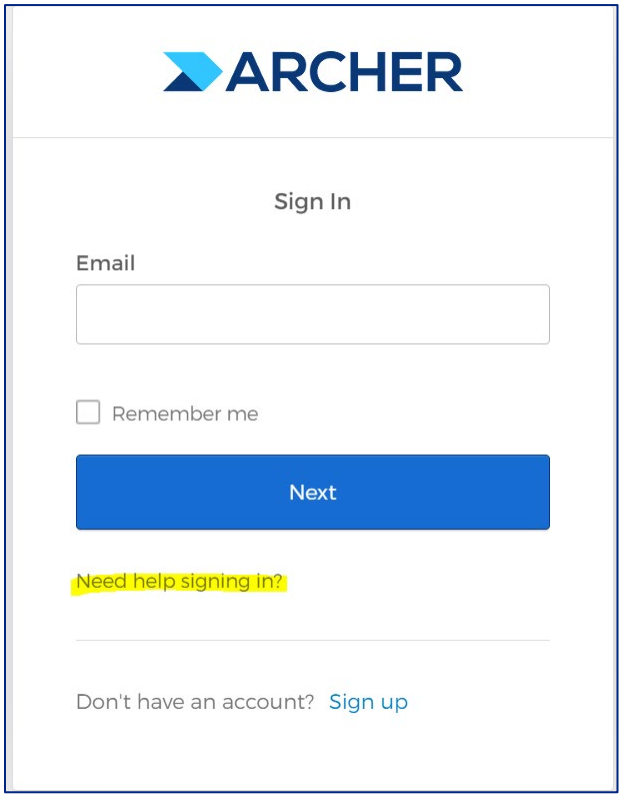
1. If you need help submitting an incident report, call (877) DIR-CISO.

Closure/Post-Mortem

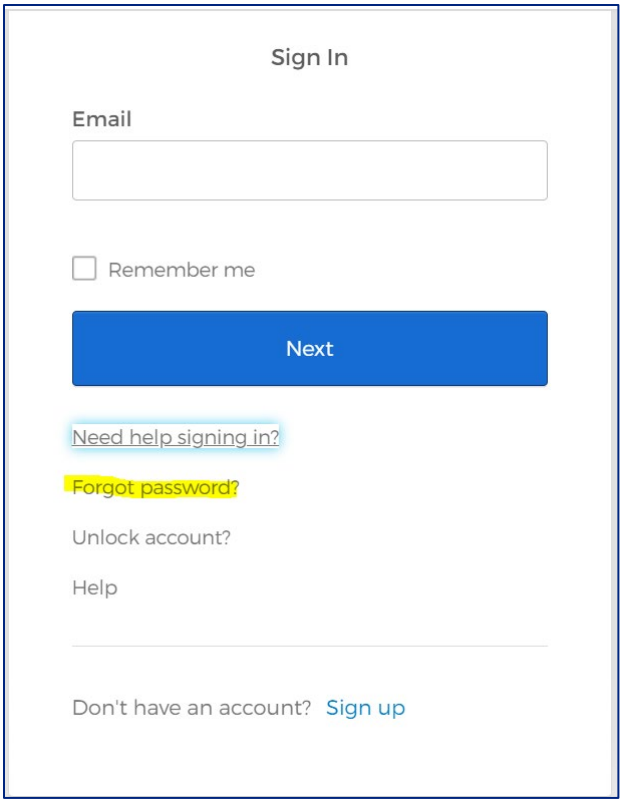
1. In addition to the original incident confirmation email, you will get a reminder email 2 weeks and 4 weeks after submitting an incident if you haven't submitted a closure/post-mortem report.
2. If you need to submit a closure/post-mortem report and don't have a copy of the incident confirmation email, contact GRC@dir.texas.gov.

Resetting Your Password

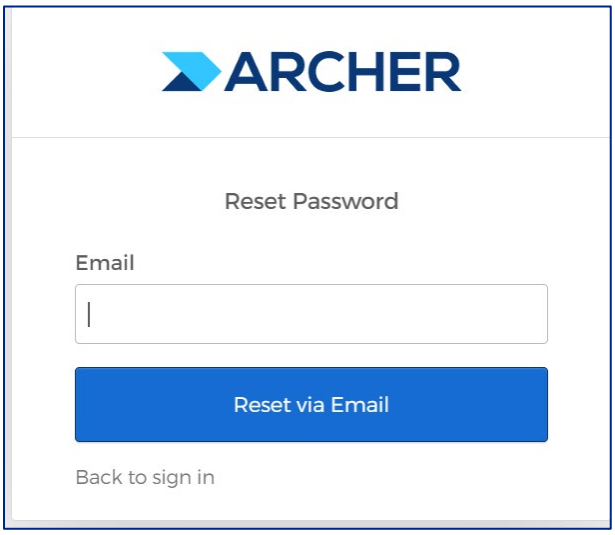
1. If you forgot your password, on the login page, click **Need help signing in?**



2. On the next screen, click **Forgot password?**



3. Then, enter your email and click **Reset via Email**.



4. Follow the instructions in the email to reset your password.

Support Requests

1. If you encounter any issues while accessing or entering an incident or closure/post-mortem report, try refreshing your screen.
2. If refreshing doesn't resolve the issue, try closing your browser and logging back in.
3. Contact GRC@dir.texas.gov if you need additional assistance. Or contact CIRT@dir.texas.gov if you need someone to submit an incident on your behalf.