# FY 23-24 Application for Security Awareness Training Program Certification

Notes:

1) A training program is a course or curriculum of courses that meets the specifications of Texas Government Code 2054.519. This is what will be certified.
2) If the training program is part of a larger set of training materials, state and local government organizations in Texas will need to include in their training program the modules/courses that are submitted for certification as a minimum to ensure compliance with state law (although they could add modules/content as desired).

I am a:

Public sector entity or vendor seeking recertification of a training program that was previously certified: Proceed to page 2

Public sector entity seeking certification on a new in-house or hybrid program: Proceed to page 6

Vendor seeking certification on a new program: Proceed to page 12

# Public Sector Entity or Vendor (Recertification)

This form is intended only for programs that were certified during Fiscal Year (FY) 22-23 and have had no changes to the previously certified content. (Program changes to address the new criteria are allowed.) If you are unsure if your program was previously certified, please consult the list of approved programs for FY 22-23.

If you are a public sector entity seeking certification on a new program, please complete the FY 23-24 public sector application for certification form.

If you are a vendor seeking certification on a new program, please complete the FY 23-24 vendor application for certification form.

Contact TXTrainingCert@dir.texas.gov with any questions about the certification process.

Additional information is available on the Statewide Cybersecurity Awareness Training webpage, https://dir.texas.gov/information-security/statewide-cybersecurity-awareness-training.

## Application Questions

### *Contact Information*

1. Organization type: State agency, Local Government, Vendor
2. Organization Name
3. Training Program Name (as certified in FY 22-23)
4. Training Program Name (for FY 23-24)
5. Primary Point of Contact for Request (who to contact for questions about the re-certification application)
    5.1. Primary POC for application (Name, Title, Email, Phone)
    5.2. Secondary POC for application (Optional)
6. Primary Point of Contact for Organization (If the training program is certified, this point of contact will be published with the list of certified programs.)
    6.1. Primary POC for organization (Name, Title, Email, Phone)
    6.2. Secondary POC for organization (Optional)

### *Content Recertification*

For FY 23-24, one new criterion has been added to the certification requirements. If there have been no changes to the content of a previously certified training program, the program can be recertified after the review of the new criterion.

I certify that there have been no changes to the previously certified content. (Program changes to address the new criteria are allowed.)

### *Program Content*

#### Mandatory Course/Program Topics

For FY 23-24, one new criterion has been added to the certification requirements. Specify where/how the criterion is addressed in the training program. Include the specific section, page and/or slide. If the training program is video-based, provide specific timestamps.

1) b) Best Practices to safeguard information and information systems.

| **Criterion** | **Where/how addressed in training program (be as specific as possible, e.g. Slide #4 in Module XYZ, or timestamp 3:45-4:05)** |
|---|---|
| v) Users should be aware of best practices related to working remotely. | |

#### Strongly Recommended Topics for IT Roles (Administrators and Management)

We strongly recommend, but do not require, that training programs with a target audience of IT roles contain the following topics.

1) Best practices for cyber hygiene.
2) Best practices for back-ups, including types, locations, frequency, testing, and protection.
3) Awareness of the Traffic Light Protocol (TLP) levels and how to follow TLP sharing guidance.

7. Does the training program include the recommended topics for IT Roles? (Yes/No)

#### Program Format and Features

We strongly recommend, but do not require, that training programs contain the following:

1) An assessment of learning outcomes.
2) Proof of completion.
3) Comply with accessibility standards: Texas Administrative Codes 1TAC 213, 1TAC 206 and/or WCAG 20.00AA or higher.
4) Phishing simulations.

8. Does the training program include an assessment of learning outcomes? (Yes/No)
9. Does the training program provide proof of completion (ex. certificate/e-certificate, completion verification email, internal tracking system/LMS, etc.)? (Yes/No)
10. Does the training program comply with accessibility standards in Texas Administrative Codes 1TAC 213, 1TAC 206 and/or WCAG 20.0AA or higher at this time? (Yes/No)
11. Does the program include phishing simulations?

### *Program Details*

12. (If State agency or local government) Program type: In-house, Hybrid

#### Additional Program Details for In-house Programs

13. Would your organization be willing to share the content of the program with other organizations? (Yes/No)

#### Additional Program Details for In-house Programs Willing to Share Content or Vendor Programs

14. Specify the target audience for the training program. (State agency, local government, K 12 school districts, other)
15. Indicate the delivery method(s) for the training program. (In-Person, Online, Files, Other – Write In)
16. Is there a cost to an organization to take the training program? (Yes/No)
17. List all languages the training program is available in.
18. Provide the estimated duration for the training program (in hours).

#### Additional Program Details for Vendor Programs

19. Is this training program within the scope of one or more DIR Cooperative Contracts to which your company is a party? (Yes/No)

    19.1. If yes, Provide the DIR Contract number(s) and your company's role (prime vendor, reseller, subcontractor) for each contract listed, e.g. DIR-TSO-XXXX, and the DIR contract manager, if known.

### *Program Submission*

Under a recertification, only the portion of the training program that addresses the new criterion needs to be submitted.

Applications for approval of security awareness training programs are not complete until training course materials are received by the DIR.

For assessment purposes:

- If providing a URL, ensure the training program is easily accessed and navigated. Provide a reviewer or similar account type that has all restrictions disabled.
- If providing a video, include a transcript file as a PDF.

20. Which of the following training course materials/supporting documentation are being provided? Select all that apply: URL, File upload-documents, File upload-videos.

    20.1. URL:

        20.1.1. Submit training program link
        20.1.2. Provide instructions and/or contact person for accessing the training program.
        20.1.3. (If applicable) Video transcript upload (DOC, XLS, DOCX, XLSX, PDF, TXT) – max 10 files, 25 MB limit

    20.2. File upload-documents:

        20.2.1. Upload documents (PNG, GIF, JPG, JPEG, DOC, XLS, DOCX, XLSX, PDF, PPT, PPTX) – max 10 files, 50 MB limit

    20.3. File upload-videos:

        20.3.1. Upload video (AVI, MOV, MP4) – max 10 files, 50 MB limit
        20.3.2. Video transcript upload (DOC, XLS, DOCX, XLSX, PDF, TXT) – max 10 files, 25 MB limit

*Certification*

21. I certify that the information I have submitted is true and complete. I understand that knowingly submitting information that is not true and complete may result in civil or criminal penalties. I acknowledge that the content of the training program will be compared against the criteria specified under Sec. 2054.519, Texas Government Code, and that the submission of this form does not in itself constitute a certification of the program.

    **Button: Submit Application**

    <<<<Thank you for your submission. You will be notified within 30 days of the determination of your training program certification status. Please contact TXTrainingCert@dir.texas.gov if you have any questions.>>

    **End Questionnaire**

# Public Sector Entity (New Program)

## Application Questions

1. Was this training program approved as a DIR certified program for FY 22-23? (Yes/No)
   1.1. If yes:

   Recertification Statement

   If this training program was approved in FY 22-23, and there have been no changes to the criteria's content, submit a Program Recertification Application, instead of an Application for Certification.

   If this training program does not meet the criteria for a recertification, continue with this application.

2. Is this a 3rd party training program? (Yes/No)
   2.1. If yes:

   Third Party Statement
   This application can be submitted for training programs developed in-house or for hybrid program programs (includes both components developed in-house and components developed by a third party).

   If this training program was developed completely by a third party, then the third party should submit the application for certification directly.

### *Contact Information*

3. Organization type: State agency, Institution of Higher Education, Junior College, Local Government/Other
4. Organization Name
5. Primary Point of Contact for Application (who to contact for questions about the certification application)

   5.1. Primary POC for application (Name, Title, Email, Phone)
   5.2. Secondary POC for application (Optional)

6. Primary Point of Contact for Organization (If the training program is certified, this point of contact will be published with the list of certified programs.)

   6.1. Primary POC for organization (Name, Title, Email, Phone)
   6.2. Secondary POC for organization (Optional)

### *Training Program Details*

A training program is a course or curriculum of courses that meets the specifications of Texas Government Code 2054.519. This is what will be certified.

If the training program is part of a larger set of training materials, state and local government organizations in Texas will need to include in their training program the modules/courses that are submitted for certification as a minimum to ensure compliance with state law (although they could add modules/content as desired).

7. Training Program Title
8. Select the type of training program. (In-house/Hybrid)
    8.1. Describe the nature of the hybrid program. Which components of the training program are covered by the third-party? Which components are covered by the organization?
    8.2. Third-party provider Name

#### Additional Program Details for In-house Programs

9. Would your organization be willing to share the content of the program with other organizations? (Yes/No)

### *Program Content*

#### Mandatory Course/Program Topics

Specify where/how each certification criterion is addressed in the training program. Include the specific section, page and/or slide. If the training program is video-based, provide specific timestamps.

10. Requirement #1: Information security habits and procedures that protect information resources

| **Criterion** | **Where/how addressed in training program (be as specific as possible, e.g. Slide #4 in Module XYZ, or timestamp 3:45-4:05)** |
|---|---|
| a) The Principles of Information Security | |
| i) Users should be aware of what 'information security' means. | |
| ii) Users should be aware of the types of information (e.g. confidential, private, sensitive, etc.) they are responsible for safeguarding. | |
| iii) Users should be aware of the forms and locations of the | |

| | |
|---|---|
| information they are responsible for safeguarding. | |

| **Criterion** | **Where/how addressed in training program (be as specific as possible, e.g. Slide #4 in Module XYZ, or timestamp 3:45-4:05)** |
|---|---|
| b) Best Practices to Safeguard Information (All Forms) and Information Systems | |
| i) Users should be aware of how to safeguard against unauthorized access to information, information systems, and secure facilities/locations. | |
| ii) Users should be aware of how to safeguard against unauthorized use of information and information systems. | |
| iii) Users should be aware of best practices related to securely storing information. | |
| iv) Users should be aware of best practices related to securely disposing and sanitizing information and information systems. | |
| v) Users should be aware of best practices related to working remotely. | |

11. Requirement #2: Best practices for detecting, assessing, reporting, and addressing information security threats

| **Criterion** | **Where/how addressed in training program (be as specific as possible, e.g. Slide #4 in Module XYZ, or timestamp 3:45-4:05)** |
|---|---|
| a) Awareness of the meaning of information security 'threat,' 'threat actor,' 'risk,' and 'attack.' | |
| i) Users should be aware of the meaning of 'threat' with | |

| | |
|---|---|
| regards to information security. | |
| ii) Users should be aware of common 'threat actors' and their motivations. | |
| iii) Users should be aware of the meaning of 'risk' with regards to information security. | |
| iv) Users should be aware of the meaning of 'attack' with regards to information security. | |

| **Criterion** | **Where/how addressed in training program (be as specific as possible, e.g. Slide #4 in Module XYZ, or timestamp 3:45-4:05)** |
|---|---|
| b) Awareness of how to identify, respond to, and report on information security threats and suspicious activity. | |
| i) Users should be aware of how to identify indicators for common attacks. | |
| ii) Users should be aware of how to respond to and report on common attacks or suspicious activity. | |
| iii) Users should be aware of the definition of spear phishing, and how to identify and report on spear phishing attempts. | |

### Strongly Recommended Topics for IT Roles (Administrators and Management)

We strongly recommend, but do not require, that training programs with a target audience of IT roles contain the following topics.

1) Best practices for cyber hygiene.
2) Best practices for back-ups, including types, locations, frequency, testing, and protection.
3) Awareness of the Traffic Light Protocol (TLP) levels and how to follow TLP sharing guidance.

12. Does the training program include the recommended topics for IT Roles? (Yes/No)

### *Program Format*

#### Program Format and Features

We strongly recommend, but do not require, that training programs contain the following:

1) An assessment of learning outcomes.
2) Proof of completion.
3) Comply with accessibility standards: Texas Administrative Codes 1TAC 213, 1TAC 206 and/or WCAG 20.00AA or higher.
4) Phishing simulations.

13. Does the training program include an assessment of learning outcomes? (Yes/No)
14. Does the training program provide proof of completion (ex. certificate/e-certificate, completion verification email, internal tracking system/LMS, etc.)? (Yes/No)
15. Does the training program comply with accessibility standards in Texas Administrative Codes 1TAC 213, 1TAC 206 and/or WCAG 20.0AA or higher at this time? (Yes/No)
16. Does the program include phishing simulations? (Yes/No)

#### Program Details for In-house Programs Willing to Share Content

17. Specify the target audience for the training program. (State agency, local government, K 12 school districts, Other)
18. Indicate the delivery method for the training program (In-Person, Online, Files, Other – please specify).
19. Is there a cost to an organization to take the training program? (Yes/No)
20. List all languages the training program is available in.
21. Provide the estimated duration for the training program (in hours).

### *Program Submission*

Applications for approval of security awareness training programs are not complete until training course materials are received by the DIR.

For assessment purposes:

- If providing a URL, ensure the training program is easily accessed and navigated. Provide a reviewer or similar account type that has all restrictions disabled.
- If providing a video, include a transcript file as a PDF.

22. Which of the following training course materials/supporting documentation are being provided? Select all that apply: URL, File upload-documents, File upload-videos.

22.1. URL:

22.1.1. Submit training program link
22.1.2. Provide instructions and/or contact person for accessing the training program.
22.1.3. (If applicable) Video transcript upload (DOC, XLS, DOCX, XLSX, PDF, TXT) – max 10 files, 25 MB limit

22.2. File upload-documents:

22.2.1. Upload documents (PNG, GIF, JPG, JPEG, DOC, XLS, DOCX, XLSX, PDF, PPT, PPTX) – max 10 files, 50 MB limit

22.3. File upload-videos:

22.3.1. Upload video (AVI, MOV, MP4) – max 10 files, 50 MB limit
22.3.2. Video transcript upload (DOC, XLS, DOCX, XLSX, PDF, TXT) – max 10 files, 25 MB limit

*Certification*

23. I certify that the information I have submitted is true and complete. I understand that knowingly submitting information that is not true and complete may result in civil or criminal penalties. I acknowledge that the content of the training program will be compared against the criteria specified under Sec. 2054.519, Texas Government Code, and that the submission of this form does not in itself constitute a certification of the program.

**Button: Submit Application**

<<<<Thank you for your submission. You will be notified within 30 days of the determination of your training program certification status. Please contact TXTrainingCert@dir.texas.gov if you have any questions.>>

**End Questionnaire**

# Vendor (New Program)

## Application Questions

1. Was this training program approved as a DIR certified program for FY 22-23? (Yes/No)
   1.1. If yes:

   Recertification Statement

   If this training program was approved in FY 22-23, and there have been no changes to the previously certified content, submit a Program Recertification Application, instead of an Application for Certification.

   If this training program does not meet the criteria for a recertification, continue with this application.

### *Contact Information*

2. Company Name
3. Primary Point of Contact for Application (who to contact for questions about the certification application)

   3.1. Primary POC for application (Name, Title, Email, Phone)
   3.2. Secondary POC for application (Optional)

4. Primary Point of Contact for Organization (If the training program is certified, this point of contact will be published with the list of certified programs.)

   4.1. Primary POC for organization (Name, Title, Email, Phone)
   4.2. Secondary POC for organization (Optional)

### *Training Program Details*

A training program is a course or curriculum of courses that meets the specifications of Texas Government Code 2054.519. This is what will be certified.

If the training program is part of a larger set of training materials, state and local government organizations in Texas will need to include in their training program the modules/courses that are submitted for certification as a minimum to ensure compliance with state law (although they could add modules/content as desired).

5. Company Website URL
6. Training Program Title

7. Is this training program within the scope of one or more DIR Cooperative Contract to which your company is a party?

   7.1. If yes, Provide the DIR Contract number(s) and your company's role (prime vendor, reseller, subcontractor) for each contract listed, e.g. DIR-TSO-XXXX, and the DIR contract manager, if known.

### *Program Content*

#### Mandatory Course/Program Topics

Specify where/how each certification criterion is addressed in the training program. Include the specific section, page and/or slide. If the training program is video-based, provide specific timestamps.

8. Requirement #1: Information security habits and procedures that protect information resources

| **Criterion** | **Where/how addressed in training program (be as specific as possible, e.g. Slide #4 in Module XYZ, or timestamp 3:45-4:05)** |
|---|---|
| a) The Principles of Information Security | |
| i) Users should be aware of what 'information security' means. | |
| ii) Users should be aware of the types of information (e.g. confidential, private, sensitive, etc.) they are responsible for safeguarding. | |
| iii) Users should be aware of the forms and locations of the information they are responsible for safeguarding. | |

| **Criterion** | **Where/how addressed in training program (be as specific as possible, e.g. Slide #4 in Module XYZ, or timestamp 3:45-4:05)** |
|---|---|
| b) Best Practices to Safeguard Information (All Forms) and Information Systems | |
| i) Users should be aware of how to safeguard against unauthorized access to information, information systems, and secure facilities/locations. | |

| | |
|---|---|
| ii) Users should be aware of how to safeguard against unauthorized use of information and information systems. | |
| iii) Users should be aware of best practices related to securely storing information. | |
| iv) Users should be aware of best practices related to securely disposing and sanitizing information and information systems. | |
| v) Users should be aware of best practices related to working remotely. | |

9. Requirement #2: Best practices for detecting, assessing, reporting, and addressing information security threats

| **Criterion** | **Where/how addressed in training program (be as specific as possible, e.g. Slide #4 in Module XYZ, or timestamp 3:45-4:05)** |
|---|---|
| a) Awareness of the meaning of information security 'threat,' 'threat actor,' 'risk,' and 'attack.' | |
| i) Users should be aware of the meaning of 'threat' with regards to information security. | |
| ii) Users should be aware of common 'threat actors' and their motivations. | |
| iii) Users should be aware of the meaning of 'risk' with regards to information security. | |
| iv) Users should be aware of the meaning of 'attack' with regards to information security. | |

| Criterion | Where/how addressed in training program (be as specific as possible, e.g. Slide #4 in Module XYZ, or timestamp 3:45-4:05) |
|---|---|
| b) Awareness of how to identify, respond to, and report on information security threats and suspicious activity. | |
| i) Users should be aware of how to identify indicators for common attacks. | |
| ii) Users should be aware of how to respond to and report on common attacks or suspicious activity. | |
| iii) Users should be aware of the definition of spear phishing, and how to identify and report on spear phishing attempts. | |

### Strongly Recommended Topics for IT Roles (Administrators and Management)

We strongly recommend, but do not require, that training programs with a target audience of IT roles contain the following topics.

1) Best practices for cyber hygiene.
2) Best practices for back-ups, including types, locations, frequency, testing, and protection.
3) Awareness of the Traffic Light Protocol (TLP) levels and how to follow TLP sharing guidance.

10. Does the training program include the recommended topics for IT Roles? (Yes/No)

### *Program Format*

### Program Format and Features

We strongly recommend, but do not require, that training programs contain the following:

1) An assessment of learning outcomes.
2) Proof of completion.
3) Comply with accessibility standards: Texas Administrative Codes 1TAC 213, 1TAC 206 and/or WCAG 20.00AA or higher.
4) Phishing simulations.

11. Does the training program include an assessment of learning outcomes? (Yes/No)

12. Does the training program provide proof of completion (ex. certificate/e-certificate, completion verification email, internal tracking system/LMS, etc.)? (Yes/No)

13. Does the training program comply with accessibility standards in Texas Administrative Codes 1TAC 213, 1TAC 206 and/or WCAG 20.0AA or higher at this time? (Yes/No)

14. Does the program include phishing simulations? (Yes/No)

### Program Details

15. Specify the target audience for the training program. (State agency, local government, K 12 school districts, Other).

16. Indicate the delivery method(s) for the training program. (In-Person, Online, Files, Other – please specify)

17. Is there a cost to an organization to take the training program? (Yes/No)

18. List all languages the training program is available in.

19. Provide the estimated duration for the training program (in hours).

#### *Program Submission*

Applications for approval of security awareness training programs are not complete until training course materials are received by the DIR.

For assessment purposes:

- If providing a URL, ensure the training program is easily accessed and navigated. Provide a reviewer or similar account type that has all restrictions disabled.
- If providing a video, include a transcript file as a PDF.

20. Which of the following training course materials/supporting documentation are being provided? Select all that apply: URL, File upload-documents, File upload-videos.

    20.1. URL:

        20.1.1. Submit training program link
        20.1.2. Provide instructions and/or contact person for accessing the training program.
        20.1.3. (If applicable) Video transcript upload (DOC, XLS, DOCX, XLSX, PDF, TXT) – max 10 files, 25 MB limit

    20.2. File upload-documents:

        20.2.1. Upload documents (PNG, GIF, JPG, JPEG, DOC, XLS, DOCX, XLSX, PDF, PPT, PPTX) – max 10 files, 50 MB limit

    20.3. File upload-videos:

        20.3.1. Upload video (AVI, MOV, MP4) – max 10 files, 50 MB limit
        20.3.2. Video transcript upload (DOC, XLS, DOCX, XLSX, PDF, TXT) – max 10 files, 25 MB limit

*Certification*

21. I certify that the information I have submitted is true and complete. I understand that knowingly submitting information that is not true and complete may result in civil or criminal penalties. I acknowledge that the content of the training program will be compared against the criteria specified under Sec. 2054.519, Texas Government Code, and that the submission of this form does not in itself constitute a certification of the program.

**Button: Submit Application**

<<<<Thank you for your submission. You will be notified within 30 days of the determination of your training program certification status. Please contact TXTrainingCert@dir.texas.gov if you have any questions.>>

**End Questionnaire**