AGENDA ITEM
CA49

AGENDA PLACEMENT FORM

(Submission Deadline – Monday, 5:00 PM before Regular Court Meetings)

Date: 09.01.26

Meeting Date: 09.14.26

Submitted By: Lance Anderson

Department: Purchasing

Signature of Elected Official/Department Head:

_____

Court Decision:
This section to be completed by County Judge's Office



9.14.2026

Description:

Consider and approve, with authorization for County Judge to sign, Texas Association of Counties Risk Management Pool Liability Renewal Questionnaire for the 18th, 249th, & 413th District Courts and CSCD.

(May attach additional sheets if necessary)

Person to Present: Lance Anderson

(Presenter must be present for the item unless the item is on the Consent Agenda)

Supporting Documentation: (check one) ☑ PUBLIC ☐ CONFIDENTIAL

(PUBLIC documentation may be made available to the public prior to the Meeting)

Estimated Length of Presentation: 5 minutes

Session Requested: (check one)

☐ Action Item ☑ Consent ☐ Workshop ☐ Executive ☐ Other _____

Check All Departments That Have Been Notified:

☑ County Attorney ☐ IT ☐ Purchasing ☐ Auditor

☐ Personnel ☐ Public Works ☐ Facilities Management

Other Department/Official (list) _____

Please List All External Persons Who Need a Copy of Signed Documents In Your Submission Email

Approved in CC on 9/11/2023

TEXAS ASSOCIATION of COUNTIES
RISK MANAGEMENT POOL

Liability Renewal Questionnaire

Member: 18th, 249th & 413th Judicial District CSCD

Coverage Period: December 1, 2026 through December 1, 2027

Thank you for participating in the TAC Risk Management Pool's Liability program. As we prepare your renewal, there are a few questions we need you to answer so that we can provide you the most comprehensive and cost effective coverage possible. Pursuant to the Interlocal Participation Agreement, Section 4. Annual Contribution, 4.01 requires that the member timely submit to the Pool documentation necessary for the Pool to properly underwrite the renewal. To ensure that we have up-to-date information, please fill out each page completely and make any changes directly to this document. You can also provide supplemental sheets as necessary. NOTE: Omitted information may result in an exclusion from coverage.

The following coverage is eligible for renewal:

- Privacy or Security Event Liability and Expense Coverage
- Public Officials Liability

We value your membership in the TAC Risk Management Pool and look forward to another successful year! If you have any questions or need help completing the Renewal Questionnaire, please contact your Member Services Representative Brittany Davis at 800-456-5974 or brittanyd@county.org.

Pool Coordinator

Our records indicate that the Member has designated the individual below as the Pool Coordinator for this coverage. In accordance with the terms of the Interlocal Participation Agreement, the Pool Coordinator has express authority to represent and to bind the Member, and the Pool will not be required to contact any other individual regarding matters arising from or related to this Agreement. If the Member wishes to change or update the Pool Coordinator information, please make the necessary changes below.

Pool Coordinator: Lance Anderson	Email: landerson@johnsoncountytx.org
Phone Number: (817) 556-6382	Fax Number: (817) 556-6385
Address: 2 N. Main St	City, State, Zip: Cleburne TX, 76033-5500

Liability Renewal Questions

1. Please update the total number of budgeted 18th, 249th & 413th Judicial District CSCD employees, including elected officials.

	Total	Airport	Hospital	
Full Time Employees:	54	0	0	Full Time = 35 or more hours per week
Part Time Employees:	4			Part Time = Less than 35 hours per week
Volunteers:	4			Volunteer = Actively serving

Privacy or Security Event Liability and Expense Coverage

Current Privacy or Security Event Liability and Expense Deductible: $10,000

To make changes to your current Privacy or Security Event Liability and Expense coverage, please complete the section below:

Coverage	Currently Included	Add to Coverage	Reject from Coverage	Current Limit	Change Limit	Limit Options
Privacy or Security Event Liability and Expense	☑			$1,000,000	☐	☐ $500,000 ☐ $1,000,000 ☐ $2,000,000
Business Interruption	☑			$250,000 / $250,000	☐	☐ $50,000 / $50,000 ☐ $250,000 / $250,000 ☐ $300,000 / $300,000 ☐ $350,000 / $350,000 ☐ $400,000 / $400,000 ☐ $450,000 / $450,000 ☐ $500,000 / $500,000
Electronic Equipment and Data Recovery	☑			$250,000 / $250,000	☐	☐ $50,000 / $50,000 ☐ $250,000 / $250,000 ☐ $300,000 / $300,000 ☐ $350,000 / $350,000 ☐ $400,000 / $400,000 ☐ $450,000 / $450,000 ☐ $500,000 / $500,000
eCrime	☑			$250,000 / $250,000	☐	☐ $25,000 / $25,000 ☐ $250,000 / $250,000 ☐ $300,000 / $300,000 ☐ $350,000 / $350,000 ☐ $400,000 / $400,000 ☐ $450,000 / $450,000 ☐ $500,000 / $500,000
Extortion	☑			$25,000 / $25,000	☐	☐ $10,000 / $10,000 ☐ $25,000 / $25,000 ☐ $30,000 / $30,000 ☐ $40,000 / $40,000 ☐ $50,000 / $50,000 ☐ $75,000 / $75,000 ☐ $100,000 / $100,000

Internal Cyber Security Point of Contact:

Name	Dan Milam	**Title**	IT Director
Telephone	817-556-6366	**Email**	dmilam@johnsoncountytx.org

Please complete all the following questions concerning the Information Technology environment within your organization. These questions are intended to be answered by an IT Director (or equivalent professional) with adequate knowledge of the organization's cybersecurity measures and protocols. All questions require completion for Privacy or Security Event Liability coverage. Increased limits will require underwriting review for consideration.

To be considered for a $1M Privacy or Security Event Liability and Expense limit the following must be met satisfactorily:

1. Our staff receive mandatory cybersecurity awareness training at least annually on expectations of staff to recognize common cyber-attacks, such as social engineering and phishing, to report possible cybersecurity incidents or other types of cyber-attacks, and to know who to report cybersecurity issues/problems to.
   - a. No, we do not receive mandatory cybersecurity awareness training annually.
   - X b. Yes, we are required to participate in mandatory cybersecurity awareness training at least annually.
2. Our staff logs in to their web-based email using multi-factor authentication (e.g., receiving a text message to validate log in).
   - X a. True
   - b. False
3. Our critical and sensitive data is backed up, stored and encrypted offline on a different logical or physical network such as a cloud backup to support recovery from a catastrophic cyber incident if required.
   - a. True, but our backups are not stored offline on a different logical network location; they are connected to our IT network, and they are encrypted.
   - X b. True, our backups are offline (in a different logical network) and encrypted.
   - c. True, our backups are offline (such as a manual hard drive backup), but they are not encrypted.
   - d. False, we do not back up our critical or sensitive data.

To be considered for a $2M Privacy or Security Event Liability and Expense limit the following must be met satisfactorily in addition to the questions noted above:

4. My organization/county has formalized IT and cybersecurity policies and plans that document, for example, guidelines for acceptable use of IT, passwords, reporting of unusual activity (e.g., workstation locking up or not functioning properly), cybersecurity training, and cyber incident response.
   - a. We have no documented policies or plans.
   - X b. We have some documented policies, procedures, and plans, but there are known gaps.
   - c. We have a robust, well documented IT and cybersecurity program that is current.
5. Our organization/county requires multi-factor authentication for remote access to our network (both cloud-hosted and on-premises, including Virtual Private Networks (VPNs))
   - X a. True
   - b. False
6. We review our organizations' IT and cybersecurity policies, procedures, and plans at least annually and we make updates/changes based on changes in the organization, the cybersecurity environment, and technology.
   - X a. True
   - b. False
7. In the case of a cybersecurity incident, we report the incident to.
   - a. Cyber Insurance Provider
   - b. Cyber Insurance Provider and Law Enforcement
   - X c. Cyber Insurance Provider, Law Enforcement, and Cyber Incident Support Vendors (may include Cyber Forensics, Cyber Legal Support, and other Cyber Incident support)
   - d. None of the Above

8. We have staff (either internal staff or outsourced contractors/vendors) who are responsible for maintaining our IT systems and applying maintenance and cybersecurity patches to software on the workstations within our organization.
    a. No, we do not have staff/contractors who perform this function.
    X b. Yes, we do have staff/contractors who perform this function.
9. We have cybersecurity tools and systems that monitor who is on our network, when they are on the network, and what network resources they are using.
    X a. True
    b. False
10. We have implemented email content filtering and web content filtering to identify unauthorized activity, malicious attachments, and other prohibited activity that may negatively impact our IT network and systems.
    X a. True
    b. False
11. We conduct interactive or simulated social engineering (i.e., KnowBe4 phishing emails) training.
    X a. True
    b. False
12. We have implemented tools (e.g., Endpoint Detection and Response tools such as Microsoft Defender for endpoints, CrowdStrike Falcon, or Malwarebytes Endpoint Security) to automatically monitor, log, and report unusual and unauthorized activities that occur on our IT workstations.
    X a. True
    b. False
13. We have software/hardware that is no longer supported by the manufacturer or vendor but is active on our IT network.
    X a. Yes, we have outdated hardware or software on our network that is no longer supported by the manufacturer or vendor.
    b. No, we do not have any hardware or software on our IT network that is no longer supported by the manufacturer or vendor.
    c. I do not know.
14. We have a formal Disaster Recovery Plan and a formal Business Continuity Plan that guides us in setting the priority of system (applications / systems / databases) restoration to recover from a cyber incident that impacts our business operations.
    a. True
    X b. False

Money Transfer Controls

15. Are employees who are responsible for disbursing or transmitting funds provided anti-fraud training, including detection of social engineering, phishing, business email compromise, and other scams, on at least an annual basis?
    X a. Yes
    b. No
16. When a vendor or supplier requests any change to its account details (including routing numbers and account numbers), do you confirm requested changes via an out-of-band authentication (a method other than the original means of request)? For example, if a request is made by email, a follow-up phone call is placed to confirm that the supplier or vendor made the request.
    X a. Yes
    b. No

Public Officials Liability

Current Public Officials Liability Deductible: $2,500

To make changes to your current Public Officials coverage, please complete the section below:

Coverage	Currently Included	Add to Coverage	Reject from Coverage	Current Limit	Change Limit	Limit Options
Public Officials Liability	☑			$2,000,000	☐	☐ $2,000,000 ☐ $3,000,000
District Attorney		☐ Add				
District Judge		☐ Add				
Back Wages - Optional Increased Limits (included coverage limit is $50,000/$100,000)		☐ Add			☐	☐ $50,000/$100,000 ☐ $100,000/$250,000 ☐ $250,000/$500,000 ☐ $500,000/$1,000,000 ☐ $1,000,000/$1,000,000

Unreported Claims

Are you, or any officer or employee, aware of, or have knowledge of any circumstance, occurrence, fact or event which is likely to be a basis of a claim, either now or in the future? Yes X **No**

If yes, please describe:

Has the situation been reported to TAC Claims Department? Yes No N/A

Acknowledgement and Acceptance

18th, 249th & 413th Judicial District CSCD (Member) acknowledges that the information submitted in this questionnaire and Auto Schedule is true and accurate, including all known potential claims. The information submitted may be used by the Pool in processing the renewal and in assessing the coverage needs of Member. The questions posed, or any wording of the questionnaire, should not and may not be relied upon by Member as implying that coverage exists for any particular claim or class of claims. The only coverage provided by the Pool to Member is as described in the applicable Coverage Document, including any endorsements and the Contribution and Coverage Declaration, issued to a covered Member.

Member acknowledges and agrees that vehicles not listed on the attached vehicle schedule, and/or additionally identified by Member as an update to the attached vehicle schedule, will not be provided coverage during the Coverage Period.

If Member makes no changes, the Pool will assume Member is requesting renewal for the same Liability Coverage as in the previous applicable Coverage Period. Member understands that any failure to fully and accurately answer the questionnaire and any attached schedules may result in denial of coverage provided by the Pool. Coverage issued for Public Officials Liability and Law Enforcement Liability will apply on a Claims Made Basis.

Signature of County Judge or presiding official of the Political Subdivision

9-14-26
Date