2023-2024 Cyber Security Matching Grant Program Guidelines

Public Entity Partners is pleased to announce the launch the 2nd annual
Cyber Security Matching Grant Program
for all members who have **general liability coverage.**

OBJECTIVE: ***To help members with general liability coverage purchase cyber security tools, training and services designed to protect the organization from ransomware and social engineering, while increasing the member's ability to qualify for the Cyber Extension Coverage.***

Cyber Security reimbursable items and services include:

- Employee training designed to assist employees in identifying and protecting sensitive information; recognizing fraudulent emails and/or emails with dangerous links, and how to recognize social engineering tactics that can lead to loss.
- Multi-Factor Authentication (MFA) for access to email, remote access to computers and servers, and access to administrative accounts;
- Data backup and disaster recovery with the requirement of storing two backup copies onto different storage media and in different off-site locations.
- Advanced Threat Protection (ATP) to protect against malware and phishing attacks, and to monitor your network and systems for abnormal or suspicious activities.
- Endpoint Detection and Response (EDR) that focuses on a single "endpoint device" (such as a server or computer). EDR looks for threats that may have infiltrated a municipality's device by watching for suspicious activity.

Please read this information in its entirety before completing the application:

1) Public Entity Partners will **reimburse up to 50 percent** of the cost of the cyber security expenditure(s) with a maximum reimbursement based on the Priority Classification matrix rating.

2) **Matching grant funds must be used for cyber security related items or training.**

3) Applicants must be an existing member and must currently have **general liability coverage** as of **7/1/2023.**

4) Applicants must be in good standing **and in compliance with previous loss control recommendations.**

PUBLIC ENTITY PARTNERS

DEADLINE: Friday, January 12th 2024 (close of business)

GRANT NOTIFICATION DATE: Week of January 29, 2024

ELIGIBILITY: Members with **General Liability Coverage** as of **July 1, 2023**. Your **expenditures** may be made between **July 1, 2022 and April 1, 2024**.

RULES FOR PARTICIPATION

1. **Applications must be submitted online**. The application is **DATE SENSITIVE** and is subject to available funds**.**

2. A signed **Resolution** or **Motion** (by the appropriate official: mayor or chairman of the board) passed by the governing body of the city/agency **MUST BE** provided. For boards of local government agencies that do not pass resolutions, a Motion is attached and may be signed by the appropriate Executive. In addition, also available on our website, please find a "fillable" Model Resolution/Motion, for your convenience.

   NOTE: If your resolution/motion cannot be approved and signed when your application is ready, you may submit the application only. However, the Resolution/Motion must be sent no later than February 29, 2024. Since the application is date sensitive, it is NOT necessary to submit the application and resolution/motion together. Please note that **y**our grant reimbursement check will not be sent to you until we have received this document.

3. Public Entity Partners will reimburse approved grants for one-half of the paid expenditures (50 percent), up to the maximum funding level for the participant's assigned classification.

4. *If* the Grant Committee approves your application, you will be asked to submit proof of payment(s) for your cyber security-related purchased item(s) before we can process your grant check. Invoices alone will NOT be used as proof of payment. **Please see Page 3 for mandatory checklist of items needed for Grant reimbursement.**

PUBLIC ENTITY PARTNERS

GRANT REIMBURSEMENT CHECKLIST:

1. **"Notification of Approval" letter**
2. **Signed Resolution/Motion**
3. **Cover sheet listing description of items purchased, quantities, and grand total of all purchases. All receipts must follow in order of the cover sheet.**
4. **Two proofs of payment which must include the following:**

    1) **CANCELLED check/bank statement OR credit card receipt/credit card statement OR Automated Clearing House (ACH) OR Automated Funds Transfer (AFT)**
    2) **Copy of invoice OR purchase order (serving as the backup to the cancelled check or credit card receipt). Submitting invoices alone will not be accepted.**

Forward all receipts/documentation to:
Tahtia Mitchell
Grant & Scholarship Program
Tmitchell@PEpartners.org
Fax: 615-371-9212

The deadline for us to receive your application and close this program is January 12th (close of business). Grant notifications will be distributed the week of January 29th, 2024.

Only ONE grant application may be approved for each town/city/agency during any given FISCAL YEAR. You may not "roll-over" an application from one fiscal year to another.

If approved for a grant, your proof of payment for expenditures must be received in this office by April 1, 2024, or your grant money WILL be awarded to the next "pending" member's application.

PLEASE NOTE : The funding for this program is limited and is time-sensitive. It is important that you are diligent in filing for reimbursement. Members who continue to submit late reimbursement receipts may jeopardize their eligibility to receive a Grant the following fiscal year. Please do not delay and plan ahead to submit reimbursement items as soon as the Approval Notification letter is received.

GRANT CONSIDERATIONS: Consideration of grants will be based on a variety of issues, such as your entity's risk management practices, loss experience, and availability of funding and submission date.

1. The primary consideration will be the amount of available funding for the fiscal year.
2. Priority will be given to risk exposures noted in the loss control site surveys, recommendations and/or loss trends, and a history of sound risk management practices.
3. Priority will also be given to expenditures related to employee sensitive information protection, cyber security & social engineering training, Data Backup, and Multi-factor Authentication.

If you need to know about your classification or if you have additional questions, please contact:

Tahtia Mitchell
Grant & Scholarship Program
Tmitchell@PEpartners.org
1-800-624-9698

Rating Classifications Funding Levels

(based upon earned general liability premium for previous year 2022-2023)

Class I — Up to $2,000

Class II -- Up to $1,500

Class III — Up to $1,000

Class IV — Up to $500

Class V — Up to $250

General Liability Coverage Classification Levels

Class I — Contributed earned premium for the previous year $100,000 or more in the requested coverage area.

Class II — Contributed earned premium for the previous year between $50,000 and $99,999 in the requested coverage area.

Class III —Contributed earned premium for the previous year between $20,000 and $49,999 in the requested coverage area.

Class IV —Contributed earned premium for the previous year between $10,000 and $19,999 in the requested coverage area.

Class V — Contributed earned premium for the previous year less than $9,999.

PUBLIC ENTITY PARTNERS

MODEL RESOLUTION
FOR GOVERNMENTAL ENTITIES

A RESOLUTION AUTHORIZING

THE CITY OF _____

TO PARTICIPATE IN

the *Cyber Security Matching Grant Program*

* *

WHEREAS, the cyber security safety of the City of _____ is of great importance; and

WHEREAS, all efforts shall be made to provide a reduced liability for the City of _____ employees; and

WHEREAS, Public Entity Partners seeks to encourage secure cyber environment by offering *Cyber Security Matching Grant Program*; and

WHEREAS, the City of _____now seeks to participate in this important program.

NOW, THEREFORE, BE IT RESOLVED BY THE COUNCIL OF THE CITY OF _____, TENNESSEE the following:

SECTION 1. That the City of _____ is hereby authorized to submit application for a *Cyber Security Matching Grant Program* through Public Entity Partners.

SECTION 2. That the City of _____ is further authorized to provide a matching sum to serve as a match for any monies provided by this grant.

Resolved this _____ day of _____ in the year of _____.

_____
Mayor

ATTEST:

_____
City Recorder

PUBLIC ENTITY PARTNERS

MODEL MOTION

FOR GOVERNMENTAL ENTITIES THAT DO NOT UTILIZE RESOLUTIONS

A MOTION AUTHORIZING

_____

TO PARTICIPATE IN
the *Cyber Security Matching Grant Program*

* *

WHEREAS, the reduced liability of _____ _____is of great importance; and

WHEREAS, all efforts shall be made to provide cyber protection for the _____.

WHEREAS, Public Entity Partners seeks to encourage a secure cyber environment by offering a *Cyber Security Matching Grant Program*; and

WHEREAS, the _____now seeks to participate in this important program.

I, therefore, move that the _____ is hereby authorized to submit application for a *Cyber Security Matching Grant Program* through Public Entity Partners; and that the _____ is further authorized to provide a matching sum to serve as a match for any monies provided by this grant.

A motion was made by _____ and properly seconded, and then passed on by the Board on _____ day of _____ in the year of _____.

_____
Appropriate Signature