**Cyber loss coverage language provided to AGRiP on April 8, 2010 by Joe DePape, Administrator of the Colorado Special Districts P&L Pool.**

**Additional Coverage I:** Data Compromise Including E-Commerce Cyber Liability

To the extent coverage is excluded by Exclusion Y, the **Pool** will pay a maximum of $200,000 per **Named Member** in any one Coverage Period for sums the **Named Member** is legally obligated to pay for:

Data Compromise:

The **Pool** will pay for **data compromise expenses** to mitigate identity theft resulting from any **personal data compromise** when legally imposed based upon the federal government’s implementation of the “Red Flag” anti-identity theft statutes and regulations and amendments thereto; upon state laws requiring notification of a security breach to everyone who could be affected by the breach, or upon similar provisions of any federal, state or local statutory law or common law.

Web Site Publishing Liability:

The **Pool** will pay for loss that the **Named Member** is legally obligated to pay as a result of wrongful acts associated with the content posted to the **Named Member’s** Web site. For purposes of this paragraph only, wrongful act is defined to include actual or alleged errors, misstatements, or misleading statements, defamation, or violation of a person’s right of privacy.

Network Security Breach Liability:

The **Pool** will pay for loss that the **Named Member** is legally obligated to pay as a result of **wrongful acts** associated with the **Named Member’s** actual or alleged neglect, breach of duty or omission in maintaining the security of the **Named Member’s** computer system.For purposes of this paragraph, computer system is defined to include systems owned by the **Named Member**, or licensed or leased by the **Named Member**. The neglect, breach of duty or omission, must allow a third party to gain unauthorized access to the **Named Member’s** computer system resulting in the publication of another’s personal information or the **Named Member’s** inadvertent transmission of a computer virus or malicious code.

Replacement or Restoration of Electronic Data:

The Pool will pay the **Named Member** the cost to recreate or restore electronic data, to pre-loss conditions, or computer programs that are damaged or destroyed as a direct result of an e-commerce incident. For purposes of this paragraph, e-commerce incident is defined as a computer virus, malicious code or denial of service attack.

Cyber Extortion Threats:

The **Pool** will pay the **Named Member** for the reimbursement of extortion threat expenses and ransom payments incurred as a direct result of cyber extortion threat. For purposes of this paragraph, cyber extortion threat is the use of a computer or other electronic communications system to obtain or attempt to obtain by threat unauthorized access to money or other financial gain, or avoidance of financial loss.

Business Income and Extra Expense:

The **Pool** will pay the actual loss of business income and/or extra expense incurred by the **Named Member** as a direct result of an e-commerce incident or cyber extortion threat.

**LIMITS:**

The most the **Pool** will pay under this Additional Coverage I is $200,000 per **Named Member** for any one Coverage Period and $1,000,000 shared all **Named** **Members** annual aggregate limit.

**DEDUCTIBLES:**

The **Named Member** will pay a $1,000 deductible per each loss or claim under this Additional Coverage I.

**EXCLUSIONS:**

Coverage under this Additional Coverage I shall not apply to the extent it is established by admission of the **Named Member** or in a final adjudication by a judge, jury or arbitrator that the liability otherwise covered under this Additional Coverage I results from any of the following:

1. Any intentional, willful, deliberate, malicious, fraudulent, dishonest or criminal act by the **Named Member**.
2. Any **claim,** act, circumstance or **occurrence,** event, transaction or **wrongful act** which took place before the inception date of this coverage form.
3. Any fines or penalties, including but not limited to fees or surcharges from affected financial institutions.
4. Defense or other expenses incurred in relation to any criminal investigations or proceedings.
5. Any virus or other malicious code that is or becomes named and recognized by MacAfee, Secunia, Symantech or other comparable third party monitors of malicious code activities and named viruses as indentified by Governmental Authorities or Information Technology Security.
6. Any failure of: data transmission lines or wireless communication connections; telephone lines; all telecommunications infrastructures equipment or facilities, and not limited to interruption in normal computer function, internet, cable, or outages to gas, water or telephone.
7. Mechanical failures including but not limited to electrical failure or electrical disruption, reduction in or surge of power, spike or blackouts.
8. Attributable to or arising out of the malfunction or failure of any satellite.
9. Arising out of any actual or alleged patent or trade secret violation, including the any actual or alleged violation of the Patent Act, the Economic Espionage Act of 1996 or the Uniform Trade Secret Act and their amendments.
10. Your reckless disregard for the security of “personally indentifying information” in your care, custody or control.