Mid Valley General Agency LLC
888 Madison St NE, Ste 100, Salem, OR 97301
Phone: 888-565-7001 ♦ Fax: 888-265-7353
quotes@midvalleyga.com

DataBreach[SM]
SUPPLEMENT FOR DATA PRIVACY AND SECURITY COVERAGE

All questions MUST be completed in full.
If space is insufficient to answer any question fully, attach a separate sheet.

I. GENERAL INFORMATION

1. Full name of Applicant: _____

II. NETWORK OPERATIONS AND BUSINESS FUNCTIONS

1. Do any of the following Higher Hazard Functions/Elements exist or take place on Applicant's network:
   (a) Monitoring, creation or control of:
      (i) Any aircraft or air-ground equipment of any kind? ..... [ ] Yes [ ] No
      (ii) Military defense system or weaponry of any kind? ..... [ ] Yes [ ] No
   (b) Process, store or transmit any:
      (i) Pornographic matter, gaming or game of chance? ..... [ ] Yes [ ] No
      (ii) Medical, dental, pharmaceutical or healthcare records? ..... [ ] Yes [ ] No
   (c) Energy, power plant, utility or pollution monitoring, supply, distribution or mapping? ..... [ ] Yes [ ] No
   (d) Any matter requiring governmental security clearance? ..... [ ] Yes [ ] No
   (e) Trade secrets relating to any client's operations? ..... [ ] Yes [ ] No
   (f) Web site host for clients? ..... [ ] Yes [ ] No
   (g) Application Service Provider for other than Applicant's own employees? ..... [ ] Yes [ ] No
   (h) Internet Service Provider for other than Applicant's own employees? ..... [ ] Yes [ ] No

III. NETWORK SECURITY
By attachment provide explanation of any No response.

A. **Basic Controls**

1. Does the Applicant:
   (a) Have written information security and acceptable use policies? ..... [ ] Yes [ ] No
      (i) If Yes, are they disseminated to all users annually or more frequently? ..... [ ] Yes [ ] No
   (b) Have either a trained staff member or outside contractor responsible for managing its information security? ..... [ ] Yes [ ] No
      (i) If Yes, which of the following applies:
      [ ] Network security only [ ] Network security and privacy compliance
   (c) Reassess its information security policy and procedures? ..... [ ] Yes [ ] No
   If Yes, how frequently: [ ] Less than annually [ ] Annually or more frequently
   (d) Securely configure firewalls, routers and other security appliances? ..... [ ] Yes [ ] No
      (i) If Yes, which of the following applies:
      [ ] Change default admin passwords [ ] Remove unneeded services
   (e) Use anti-virus and anti-spyware software? ..... [ ] Yes [ ] No
      (i) If Yes, which of the following applies:
      [ ] On all desktop computers with automatic update
      [ ] On all computers and servers with automatic update
      [ ] Scanning all incoming email

2. How does the Applicant manage its:
   (a) Security patch notifications from its major systems vendors? [ ] No automatic notice
   [ ] Automatic notice (where available) and implement in more than 30 days
   [ ] Automatic notice (where available) implement in 30 days or less
   (b) Change control process to ensure that modifications to its network do not compromise security before implementing them in production? [ ] No security testing
   [ ] Some upgrades subject to security testing [ ] All upgrades subject to security testing

3. How does the Applicant limit access to its network? [ ] No controls or use shared log on ID's
   [ ] Unique user ID's [ ] Unique user ID's and role based access to sensitive data

4. Does the Applicant have a process to delete systems access within 48 hours of employee termination? ..... [ ] Yes [ ] No

5. Does the Applicant perform background checks on all employees and contractors with access to parts of its network that contain sensitive data? ..... [ ] Yes [ ] No

6. Is sensitive data in databases, logs, files, backup media, etc. stored securely for example by means of encryption or truncation? ..... [ ] Yes [ ] No

7. Does the Applicant store sensitive information on any of the following media? If Yes, is it encrypted?

	Sensitive Data	Encrypted
(a) Laptop hard drives?	[ ] Yes [ ] No	[ ] Yes [ ] No
(b) PDA's / other mobile devices?	[ ] Yes [ ] No	[ ] Yes [ ] No
(c) Flash drives or other portable storage devices?	[ ] Yes [ ] No	[ ] Yes [ ] No
(d) Back-up tapes	[ ] Yes [ ] No	[ ] Yes [ ] No

8. Is encryption used in the transmission of sensitive information via e-mail? ..... [ ] Yes [ ] No

9. How does the Applicant:
   (a) Log access attempts to its network? [ ] No log [ ] Log unsuccessful attempts only [ ] Log all attempts
   (b) Audit access to sensitive information by authorized users? [ ] No audits [ ] In response to incidents
   [ ] Random audits quarterly or more frequently

10. Is access to equipment, such as servers and workstations, and storage media containing sensitive data physically protected? ..... [ ] Yes [ ] No
    If Yes, how is it physically controlled? [ ] Areas open to employees only [ ] Role based access controls

11. Does the Applicant ensure sensitive data is permanently removed (e.g., degaussing, overwriting with 1's and 0's, physical destruction but not merely deleting) from hard drives and other storage media before equipment is discarded or sold and from paper records prior to disposal? ..... [ ] Yes [ ] No
    If Yes, how is data permanently removed? [ ] Paper records with sensitive data shredded
    [ ] Data permanently removed before equipment sold or discarded

12. Is a vulnerability scan or penetration test performed on all Internet-facing applications and systems before they go into production and at least quarterly thereafter? ..... [ ] Yes [ ] No

13. Is an intrusion detection or intrusion prevention system used in the Applicant's network? ..... [ ] Yes [ ] No

14. Are security alerts from the intrusion detection or intrusion prevention system (IDS/IPS) continuously monitored and are the latest IDS/IPS signatures installed? ..... [ ] Yes [ ] No

15. Are there regular internal or external audit reviews of the Applicant's network? ..... [ ] Yes [ ] No
    If Yes, attach a copy of the last examination/audit of the Applicant's network operations, security and internal control procedures, PCI or HIPAA compliance.

B. **Collection or Storage of Sensitive Information on Web Sites & Servers**
Check if not applicable. [ ]

1. Does the Applicant require individual user ID's and passwords for any areas of your web site where sensitive data is collected? ..... [ ] Yes [ ] No

2. Are all sessions where sensitive data is entered encrypted with a Secure Socket Layer (SSL)? ..... [ ] Yes [ ] No

3. Does the Applicant have any sensitive data on its web server or on any device connected to its web server? ..... [ ] Yes [ ] No
   If Yes, is this data encrypted? ..... [ ] Yes [ ] No

4. In the development of the Applicant's web applications, has the Applicant adopted Open Web Application Security Project (OWASP) or other best practices to defend against known web attacks (Cross Scripting, SQL Injection, etc.)? ..... [ ] Yes [ ] No

C. **Wireless and Remote Access to Applicant's Network**
Check if not applicable. [ ]

1. Does the Applicant secure remote access to its network? ..... [ ] Yes [ ] No
   If Yes,
   [ ] ID/password only [ ] VPN or equivalent [ ] VPN or equivalent with two factor authentication
   [ ] No remote access

2. Does the Applicant require minimum security standards (anti-virus, firewall, etc.) for any computers used to access the network remotely? ..... [ ] Yes [ ] No

3. Are all wireless access points to the Applicant's network encrypted with WPA/WPA2 or more recent standard (e.g., not unencrypted or using WEP standard)? ..... [ ] Yes [ ] No

4. Is there a firewall between all wireless access points and the parts of your network on which sensitive information is stored? ..... [ ] Yes [ ] No

5. Does the Applicant have a repeatable process to identify rogue/unauthorized wireless devices connected to its wireless network? ..... [ ] Yes [ ] No

D. **Payment (Credit and Debit) Card Handling**
Check if not applicable. [ ]

1. Does the Applicant:
   (a) Store any payment card information on its network? ..... [ ] Yes [ ] No
      (i) If Yes, is it for one time use or does the Applicant retain it for re-use or regular subscription/installment payments? [ ] One time use [ ] Retain at least some for future use
      (ii) Is it masked, encrypted and purged in compliance with PCI standards? ..... [ ] Yes [ ] No

2. Does the Applicant process any payment card transaction over wireless networks? ..... [ ] Yes [ ] No

3. Does the Applicant store Card Security Code/Card Verification Value (CSC/CVV) data on its network? ..... [ ] Yes [ ] No

4. Is the Applicant certified as complying with the applicable PCI standard? ..... [ ] Yes [ ] No
If Yes, indicate the person or outside firm which certified the Applicant and the date of the last PCI audit. _____

IV. NETWORK SECURITY INCIDENT AND LOSS HISTORY

1. Has the Applicant at any time during the past three (3) years had any incidents, claims or suits involving unauthorized access, intrusion, breach, compromise, or misuse of the Applicant's network, including embezzlement, fraud, theft of proprietary information, denial of service, electronic vandalism or sabotage, computer virus or other incident whether or not reported to its insurance carrier? ..... [ ] Yes [ ] No
If Yes, attach a separate document describing each incident including the cause, internal costs, cost to third parties, length of time involved in recovery and steps taken to mitigate exposure in the future.

2. Is the Applicant or any of its principals, partners, officers, directors, managers, managing members, or employees, its predecessors, subsidiaries, affiliates or any other person or organization proposed for this insurance aware of any circumstance related to its network operations which might give rise to a loss or a claim? ..... [ ] Yes [ ] No
   (a) If Yes, provide full details: _____

3. Has any application for similar insurance made on behalf of the Applicant, its predecessors, subsidiaries, affiliates, and/or for any other person(s) or organization(s) proposed for this insurance ever been declined, cancelled or nonrenewed? ..... [ ] Yes [ ] No
   (a) If Yes, provide full details: _____

Signing this Supplement does not bind the Company to provide or the Applicant to purchase the insurance.

It is understood that information submitted herein becomes a part of the application for insurance and is subject to the same declarations, representations and conditions.

Must be signed by director, executive officer, partner or equivalent within 60 days of the proposed effective date.

Name of Applicant	Title (Officer, partner, etc.)
Signature of Applicant	Date