avant SUPERMARKET GROUP℠
Division of Specialty Program Group, LLC

Data Breach Questionnaire

Ph# (816) 251-1670 Fax# (816) 866-9223
submissions@avantsupermarketgroup.com

Data Breach Questionnaire is required prior to any quote release.
Please complete all sections or mark N/A if not applicable.

Insured: _____Web Address: _____

Mailing Address: _____

Agent: _____

General Security/Confidentiality Practices

	Yes	*No*	*N/A*
1. Do you store, manage, utilize, transmit or otherwise handle Private Identifying Information such as Social Security Numbers, Credit Card Numbers, Bank Account Numbers, etc… on:			
Employees……			
Vendors……			
Customers……			
Approx. No. of records kept: ☐<5k ☐ 5-25k ☐ 25-50k ☐50-250k ☐ >250k			
% Electronic:_____ % Paper_____			
2. Do you pull or use credit bureau data on a regular basis? If yes describe below……..			
3. Do you comply with Payment Card Industry (PCI) standards?.....			
4. A Compliance Officer has been designated to ensure compliance with established institutional standards for handling data……			
5. A written Data Security protocol has been established and shared with all employees?.....			
6. Is this Data Security protocol updated at least bi annually?.....			
7. Employee background checks, including criminal background checks, are completed on employees who will have access to Private Personal Data?.....			
8. Employees sign confidentiality agreements?.....			
9. Specific Data Security training which includes specific sanctions up to termination for data security violations is given to all employees?.....			
10. Access to data files are restricted to specific project staff?.....			
11. Written and explicit policies are in place to deal with a Data Breach?.....			
12. The security practices of the firm have been audited without findings of deficiencies……..			
If deficiencies identified, please detail the deficiencies and resolution on a separate sheet			

Electronic Security Practices

	Yes	*No*	*N/A*
1. All users with access to systems are authenticated by means of unique and individually assigned passwords, biometrics or digital ID……			
2. Access is controlled by role based authentication and an internal firewall……			
3. An audit trail that documents user activity is maintained……...			
4. Firewalls, Spam Filters, Virus Protection etc. are used and updated at least quarterly……..			
5. Data that is sent, received and/or stored electronically is encrypted with the highest available encryption software?.....			
6. A specific data retention/destruction schedule is adhered to. Describe protocol below…….			
7. Do you permit Private Personal Data stored on electronic devices (i.e. laptop, PDA, etc…) to be removed from your premises? If yes, describe authorization & control measures below…			
8. Do all the same internal on site security measures (physical, electronic and procedural) apply to off site or virtual employees?.....			

9. Written data back-up and disaster recovery plan is created and adhered to……..			
10. Do you require your service providers to maintain at least the same level of data security regimen that you maintain……..			
11. Does your company utilize any Wireless Networking technology in your business?.....			
12. Does your company allow use of file sharing or Peer to Peer networking technology?.....			

Paper Record Security Practices

	Yes	*No*	*N/A*
1. Do you have secure storage areas (i.e. locked rooms, locked file cabinets, limited access areas, etc…) for documents containing customer and/or employee personal identification information?.....			
2. Is access to such info restricted to only need to know employees?.....			
3. Do you have a sign out procedure when documents are removed from such areas?.....			
4. Do you have a written procedure for the secure transport of documents from one location to another?.....			
5. Do you have a regular document destruction policy…….			
6. Do you supply shredding facilities/capabilities for paper documents ……..			
7. Do you outsource paper shredding and document destruction functions to 3rd parties….			
8. Do you have pre coded dialing numbers in fax machines used for sending personal information?.....			
9. Do you restrict the removal of paper documents containing personal identification information from your premises?.....			
10. Is the personal identification information of customers, employees, etc. regularly sent out via mail, FedEx, UPS, or other delivery service?.....			

Breach History

Describe any previous breaches and the steps taken to correct deficiencies:

_____
_____
_____
_____

Describe any particular security measures your firm employs (including use of security consulting firms, etc…).

_____
_____
_____
_____

Additional Clarification/Comments_____

_____
_____
_____
_____
_____
_____
_____

Signature of Applicant: _____ Date: _____