Ann Arbor Insurance Centre

How we **PROTECT** you...

Ann Arbor Insurance Centre takes the security of the information that you entrust to us very seriously. This sheet provides a very brief overview of some of the efforts that we take to ensure that your information will be safe with our company.

Network Protection - Firewalls at all entry points into our network allow only whitelisted traffic into our network. Our firewalls also apply web-filtering, intrusion protection, anti-virus scanning, and logging of all traffic.

Data Encryption - Any time data travels over a non-secure medium, such as the Internet, it is encrypted. This includes emails with confidential information, data in transit to our vendors, data in transit to our backup sites, and delivery of data to our auditors and regulators.

Data Destruction - All confidential data is destroyed in a secure manner. This includes data on paper, which is shredded on-site, as well as electronic data.

Access to Data - We provide access to information systems on a need to know basis. Access is provided under dual-control: a manager authorizes system access, and IT grants this access. All systems require successful authentication prior to accessing information.

Password Controls - Systems are configured to require strong passwords. Employees are trained on how to select strong passwords, and how to protect these passwords.

Vendor Management - We use a detailed vendor management program that involves rating the risk associated with each vendor relationship, and evaluating the controls each vendor has to protect the data that we share with them on an annual basis.

Governance - Our corporate IT Steering Committee provides oversight for all IT activities, including policy development and exceptions, security, training, testing, and risk assessments.

Training - All employees at our company receive information security training at hire and annually thereafter. Training is tailored to the threats and issues seen each year.

Testing - We test the controls that we have in place throughout the year. This includes quarterly vulnerability testing of our network, annual information security audits, an annual social engineering testing. Any issues are remediated in a timely basis to strengthen our overall security posture.

Policies - We have a detailed and comprehensive information security program and policies. This program includes policies for incident response, patch management, electronic data retention, and vendor management, among others.

Physical Security - Our server rooms are secured such that only authorized IT personnel may enter. Paper with confidential information is secured each night, and our offices are protected with security systems.