AMINA

Fact Sheet MX1-03

Data Protection Self Assessment

Can you answer *yes* to any of these questions?

- ❑ Does your company engage contractors or third party suppliers?
- ❑ Does anyone in your company use texting, blogging, or social networking?
- ❑ Does your company accept payment by credit card?
- ❑ Do your employees surf the Internet for purposes that are not work-related?
- ❑ Do people who work at your company carry a USB thumb drive, wireless device, or cell phone?
- ❑ Does your company hold or have access to medical information about anyone?
- ❑ Would employees, investors, customers, or donors be upset if their personal information was leaked from your company?
- ❑ Does anyone use remote access to log onto your company systems?
- ❑ Does your company have any personal information about employees, contractors, or customers?
- ❑ Do suppliers, vendors, or maintenance personnel enter your company premises?

If you answered ***Yes*** to any of these questions, you might be at risk — and you might not realize it.

Can you answer *no* to any of these questions?

- ❑ Are you certain that your company's information systems have not been compromised?
- ❑ Do you know what indirect costs could result from an information breach?
- ❑ Are all of your company's critical processes and applications documented clearly?
- ❑ Are you certain that controls limit access to data only to those who have a legitimate need to know?
- ❑ Has a security clearance check been done for employees and contractors who have access to your company's premises and information systems?
- ❑ Do you have current and complete Information Privacy and Data Handling policies in place?
- ❑ Do you have an ongoing privacy awareness program that regularly teaches concepts and best practices to staff and contractors?
- ❑ Are you certain that unauthorized off-site wireless devices cannot penetrate your systems?
- ❑ Are you certain that the virus protection on your remote workers' laptops, tablets, and smartphones is up-to-date?
- ❑ Are your company's access control lists kept current?

If you answered ***No*** to any of these questions, your company, employees, investors, and stakeholders are probably at risk.

Do you know the answers to these questions?

- ❑ How can privacy planning increase profitability?
- ❑ Which international privacy or data protection laws affect your company?
- ❑ Would your insurance cover losses arising from cyber risks?
- ❑ Could your company survive the indirect costs of even one breach — regardless whether the breach is real or rumor?
- ❑ Can sending joke email result in a lawsuit?
- ❑ What would happen if investors thought their personal information was leaked from your company?
- ❑ Do all users know what data privacy and protection policies are in effect at your company?
- ❑ Which employees really need to see sensitive data to do their jobs?
- ❑ What would happen if your competitors gained access to confidential corporate data?
- ❑ Does every remote user have up-to-date firewall and security protection on the computer they use to connect to your systems?

If you ***Don't Know*** the answer to any of these questions then your organization, its employees and stakeholders are at risk.

Suite 330 Unit 440 | 10816 Macleod Trail SE | Calgary Alberta Canada T2J 5N8 | Telephone 403.254.4376 | info@AMINAcorp.ca