Tips to Help You Keep Your Company/Customer Information Safe

Aside from protecting your restaurants with applicable insurance, you can also protect yourself by using a few simple strategies:

- Form a risk assessment team to examine your network's infrastructure or hire a vendor to test your system's integrity. Identify areas of vulnerability. If you don't have even basic measures such as firewalls and virus protection software installed, you'll need to get them. Keep in mind that even these measures will not completely eliminate the threat of an attack, as hackers are constantly finding new ways to deliver cyber perils such as Trojan Horses, worms, viruses, malware, spyware and denial of service attacks.
- Monitor cameras for suspicious Employee/Customer behaviors. Camera providers like Westec will monitor for you.
- Keep backup files on a stand-alone system that is never connected to the internet to ease the data restoration process. If paper files are kept, be sure they are always secured. For example, emp info, credit card receipts, etc.
- Disable non-essential network services and eliminate software that employees do not need to do their jobs.
- Update antivirus programs, security software and operating systems regularly to reduce the possibility of an intrusion.
- Make sure to examine your business property and liability policies to avoid overlaps in coverage for electronic data loss and privacy invasion.
- Implement a company-wide security policy that establishes safety practices such as strong employee passwords that change every quarter.
- Change your password regularly and create passwords difficult to guess (numbers, special symbols, etc.)
- Don’t give anyone’s information out online, via email, text message, etc. Simply because they are convincing, verify the source for the request first.
- Have your bank authorize checks or wires of a certain amount. This will help to prevent someone from finding your bank password and wiring all the money out.
- If you discover a breach, it is your responsibility to notify possible victims and protect your company from any further attacks. Depending on regulation in your state, you may also be responsible to provide a call center of credit monitoring for those affected. Remember, regulations depend on the state in which they reside, not the state where your restaurant is located.
- Restrict access to personal information records to only those employee’s who need access to perform their duties
- **Tighten** internal electronic data access control. Information only provided to employees only on the basis of need.
- **Destroy,** on a regular maintenance schedule, older stored data that is no longer deemed necessary. Consult with your attorney and your accountant to develop guidelines and a schedule so that deletions conform to legal and accounting requirements.
- **Monitor** employees' electronic activity and investigate abnormal behavior. Look for access during non-work hours, large downloads and employees who obtain information that may not be required.
- **Proactively track** who is accessing what information on the network. Compare the activity to what individuals should be accessing. Many organizations also scan outgoing and incoming e-mail. Audit the information employees are accessing remotely and the data being turned over to outsiders, third-party individuals, companies and contractors.
- **Overlap** the responsibilities of multiple employees, who work with (or have access to) sensitive data, so they can observe each other's activities. This would be similar to having two or more employees overlapping in dealing with financial recordkeeping to decrease the opportunities for embezzlement.
- Having multiple employees overlapping duties is a must for any organization committed to data security. No one person in the team should have sole responsibility for a given system, platform or application. This requires cross-training of individuals and ensuring that the individuals regularly rotate responsibilities.
- **Adopt** written policies and procedures about use of, and access to, your electronic and digital equipment and systems. The policies and procedures need to deal with what is allowed, what is prohibited, and the consequences if an employee misuses or wrongfully distributes information, records, and documents. Distribute the policies and procedures to all employees and obtain their signatures verifying they received, read, and understand the policies.
- **State clearly** in the policies that former employees will no longer have access to private, sensitive, and confidential information. This especially means that former employees are not given access to employer-issued or employer-owned computers, laptops, other data-bearing devices, or paper documents.
- **Communicate regularly**, at least once a year, these policies and procedures to all employees.
- **Establish and nurture** a culture of trust and fairness among employees. **Develop** hiring procedures that:
    - *Attract* the kinds of people who want to work for you and who want to perform well in their jobs.
    - *Place* the people in the jobs they are most qualified to do. By matching the right applicants (those with values and expectations that fit your culture) to the right jobs (that make use of their talents), you increase the chances employees are engaged in their work and loyal to your organization.

Please contact McDonald’s Corp. for further information, advice, and insurance providers.
See next page for Disclaimers

Disclaimer of Liability

Our firm provides the information for general guidance only, and does not constitute the provision of advice, or professional consulting of any kind. The information provided herein should not be used as a substitute for consultation with security professionals, legal, or other competent advisers. Before making any decision or taking any action, you should consult a professional adviser who has been provided with all pertinent facts relevant to your particular situation. The information is provided "as is," with no assurance or guarantee of completeness, accuracy, or timeliness of the information, and without warranty of any kind, express or implied, including but not limited to warranties of performance, merchantability, and fitness for a particular purpose.