CYBER SECURITY *checklist*

CITYNET®

SOFTWARE

Are you keeping your operating systems updated? Do you monitor for operating system (OS) issues and have your OS set for automatic updates?	Stay current with the latest security patches and updates. Turning off computers at night or rebooting equipment/devices helps with the installation of updates.
Do you regularly update your anti-malware?	Make sure your anti-malware programs are set to check for updates frequently and scan devices on a set, automatic schedule along with any media that is inserted (USB thumb and external hard drives) into a workstation.
Do you perform regular, automatic, offsite backup of data?	Data protection is paramount to business continuity and customer protection. Make sure all backups are up-to-date and usable. Review backup logs and restore files randomly to make sure they work as required. Having multiple types of backups is wise, such as remote storage as well as local, physical backup. Ransomware can attack backups, so also having a method of backing up to local storage and then disconnecting from the Internet is an additional strategy. Today's threat landscape is complicated, and you must consider data backup and protection from multiple angles. Citynet can help you with a sound data protection strategy.

PEOPLE

Do you minimize administrator privileges?	Allowing workstations to run in administrator mode exposes that machine to more security threats and can lead to the entire network being infected, so regular work should NOT be done on a computer in administrative mode, which IT should disable by default.
Do you provide security awareness training for employees?	This is crucial and the first step in your security plan. Your employees are you first line of defense against a multitude of growing threats. While this training was once considered a good practice to do every year, consider conducting it every quarter as new threats grow each day. This training would include how to protect against nefarious phishing and pharming, and ransomware and social engineering threats used by hackers to get access to your important data. Citynet requires all its employees to undergo this training every quarter. Citynet can set up this informative, dynamic, and even fun online training for your team from our security training partner, KnowBe4.
Do you screen potential employees and independent contractors?	Make sure you complete a thorough background check on all potential employees or independent contractors before allowing them access to your resources. With today's Internet connectivity and tiny USB storage devices, thousands of files can be covertly copied in minutes without anyone else realizing it.
Do you pay attention to and greet all office visitors?	As you will learn in your security awareness training, social engineering, a tactic used in person to steal data, is often overlooked. Make sure employees interact with anyone that is in the office that they don't recognize and stay with them until they are with the person to whom they are to meet. If the visitor seems suspicious, notify a superior immediately.

POLICIES, TRAINING & INSURANCE

Do you have a strong password policy or require the use of an approved password manager?	Your IT policy (you have one, right?) should mandate complex passwords, meaning at least eight characters with a combination of upper and lower-case letters, numbers and special characters. Network settings should require personnel change their passwords at least four times per year and staff should not be able to reuse previous passwords. Use different passwords for each login and not allowing anyone to know your password.
Do you have a policy for protecting mobile gear?	Make sure that company laptops, tablets and smartphones utilize strong passwords and encryption. Make sure your IT policy requires staff to notify management or IT personnel if a device is stolen or misplaced so that all data on it can be erased remotely.
Do you have an IT policy?	IT policies are not just for large companies. It does not need to be complex but should address core security threats and requirements for mitigating them. Beyond including the basic computer and internet usage policies, also include BYOD (Bring Your Own Device), remote access, privacy, and encryption practices where appropriate. Citynet can help you craft such a policy as well as provide easy to deploy and budget friendly solutions to make incorporating IT requirements and compliance easier by your team.
Do you regularly review and update IT Policies?	Number one of course is making sure to have an IT policy. Then, make sure to regularly review it as threats and new solutions and best practices for fighting them are constantly evolving. Make sure to have employees review the policy and sign off on it regularly as well.

EMERGENCY

Do you have a breach response plan?	Imagine the worst-case scenario – your network security has been breached somehow – maybe you were the victim of ransomware. Now what? You must have a security incident response plan in place so that wherever company data or security has been compromised you know what to do. Such a plan should be in a written format that would include directing your personnel on how to document the events leading up to the breach discovery, notifying appropriate company/external IT personnel of the breach so they can take necessary steps to stop it, and the steps for an internal and external communications plan.
Do you have cybersecurity insurance?	You can do all the right things and yet still suffer a cyber-attack, so consider cybersecurity insurance. This is becoming a popular type of insurance for businesses and the cost for it has come down over the years. Investigate both first-party insurance to cover direct losses resulting from the breach (downtime, the recreation of data, direct remediation costs) and third-party insurance to cover any damages to customers or others whose data may have been compromised.
Do you outsource any or all of your cyber-security to experts?	Whether you have IT expertise, or even if you have IT professionals on your staff, consider outsourcing some if not all of your IT. Today's digital landscape is complex and ever-changing. Outsourcing IT doesn't have to replace your internal team, but it can allow them to focus on other areas of technology and support while your outsourcing partner can manage dynamic solutions to protect and mitigate the overall threat matrix, in tandem with your team or as a stand-alone security team at your service. Your outsourced security provider will have experts who undergo constant training and obtain professional certifications in the latest trends and solutions. These experts have likely encountered a vast array of cybersecurity issues and can put that knowledge to work for your benefit.

EQUIPMENT & DEVICES

Are you deploying mobile security tactics?	Make sure employees have secure access to your network, from any device, anytime with a secure VPN like Cisco's Any Connect.
Do you require employees to connect securely to the company network?	You should require staff to connect securely to your network resources by utilizing a VPN (virtual private network). An easy solution is to require a solution such as Cisco's AnyConnect which requires employees to utilize it to make such a connection – and it can be used in conjunction with a multi-factor authentication solution for additional security.
Are you and your staff using two-factor (TFA) or multi-factor authentication (MFA)?	If this isn't already a standard and required tactic for your business, it should be. A TFA/MFA solution such as Cisco's DUO is a critical step toward securing access to your network and applications.
Do your employees have their phones/devices set for automatic updates?	
Are you utilizing the automatic screen lock feature on computers/devices?	When a workstation or mobile device has been idle for a few minutes, make sure it's set to automatically lock the screen to keep out unauthorized access.
Do you track and tag your digital equipment?	Make sure you know where your digital equipment is located, and to whom it is assigned. This not only includes computers and servers, but all devices, thumb drives, backups and cloud services utilized by your company. Assign digital assets and access resources to only those who require it.
Do you secure your devices?	Any device that contains company and customer information needs to be physically or digitally secured. On-premise file servers need to be in a locked room/cage and the office should have a security system. Mobile devices need to be locked when not in use and any data drives encrypted.
Do you require employees to have proper security on their personal devices that are sometimes (or always) used for company work?	Making sure that your network is protected means making sure all with access to it connect securely and protect their personal devices they use when connecting to it. An infected personal device that then connects to your business network creates a threat.
Do you dispose of data/equipment properly?	Place all sensitive physical files with company or customer information in a secure area, such as a locked trash cabinet and then be sure to shred this information. There are organizations that will give you a secure waste can and when full, will come and have it securely shredded for you. Workstations and other mobile equipment used for business must be thoroughly reformatted or have the hard drive physically destroyed to minimize the risk of data compromise.