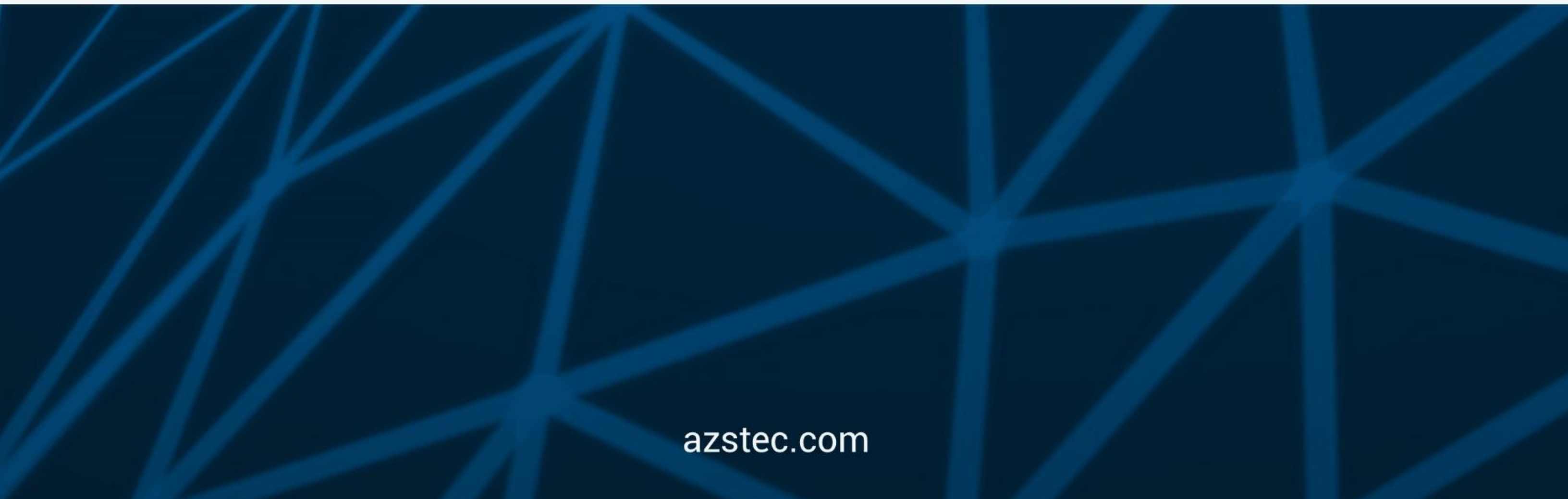
AZSTEC

CYBERSECURITY WORKBOOK

COMMON SENSE SECURITY ROADMAP
FOR SMALL BUSINESSES



azstec.com

TABLE OF CONTENTS

1. Introduction

This cybersecurity workbook was developed by Azstec LLC to assist small businesses in implementing common sense processes and procedures to minimize cybersecurity risks. While we have included information for developing a comprehensive plan, we've also included a short list of the most important areas for you to focus on to protect your business in 2016.

Resources for developing a comprehensive cybersecurity policy are listed in Appendix 3 at the end of this workbook and, of these, we believe the best template to use is ISO/IEC27002. This guideline is admittedly more detailed than most small companies need but it provides an excellent and comprehensive model for developing a company specific plan.

Let's first take a look at what a small company's infrastructure might look like.

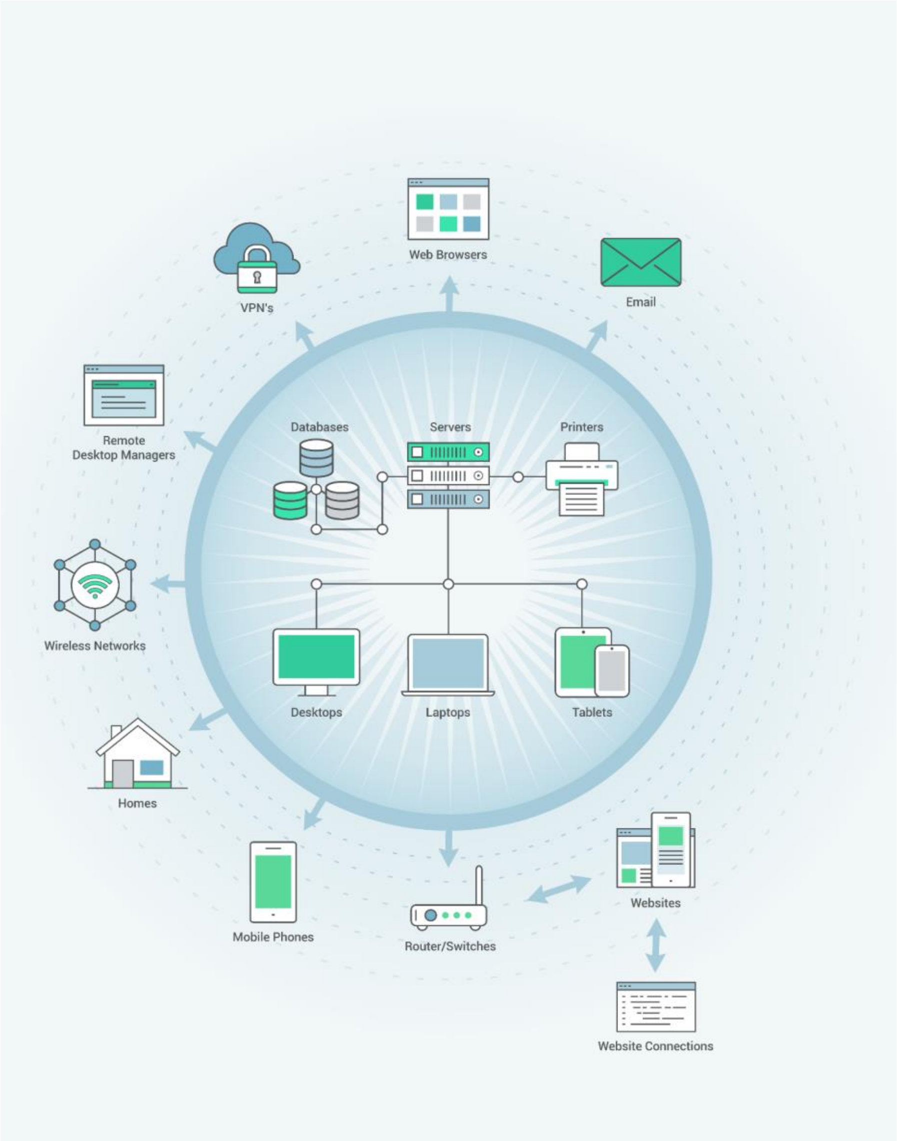


Diagram 1. A typical small business connectivity environment.

The diagram above illustrates a typical small business connectivity environment. Since a policy guideline like the ISO/IEC27002 might be intimidating, it’s easier to think about your infrastructure visually to identify the critical areas you need to secure and then branch out into other areas that may have less security risk associated with them.

The first area of concern should be the perimeter to your network. Most companies today have some form of hardware and software firewalls in place and this bridge between your network and the outside world is the first area that you need to make sure is secure. Is your firewall correctly configured? What rules are in place for blocking unwanted incoming and outgoing traffic? Are alerts being sent to the network manager?

Once you‘ve reviewed your firewall systems you should look for other places where hackers might be able to breach your network. In most small company networks the highest risk areas for unauthorized access are:

1. Email
2. Browsers accessing remote Web content
3. Wireless network connections
4. Remote desktop services
5. Removable storage (USB drives and flash drives)
6. Virtual Private Networks (VPNs)

It’s likely that your website is located outside your IT infrastructure. Key customer or other contact data on this site as well as the connection between your in-house operation and your Web server need protection. Credit card data is particularly sensitive and subject to Payment Card Industry (PCI) compliance. Given the complexity of commercial Web properties you might need the services of a security consultant to get a thorough review of your site.

Another area of vulnerability is remote workers. With the growing trend for working from home and mobile access, you need to evaluate the security of those connections as well as that of the devices used. The fact is that with the increase of the home office worker your security policy will have to extend into the previously considered private infrastructure of our employees.

If you secure your perimeter and follow our advice to encrypt all confidential data you will be well on the way to effectively protecting your sensitive information and, in turn, your company.

Before we get into what a basic plan should look like, let’s first take a look at the major areas covered in a comprehensive plan.

2. Cybersecurity Policy Overview

As discussed above, when you're building a security plan we suggest you use the ISO/IEC 27002 document as a model to help find the areas of potential weakness within your organization as well as identify areas you may not have considered. If you already have a cybersecurity program, it will help you identify what gaps you may have in your current plan.

The ISO document is comprehensive and reasonably priced. In addition to ISO, another excellent source of information is the SANS Institute. All of the SANS material is free to use and available to anyone. In Appendix 3 we have included information on where to find both the ISO and SANS material as well as additional resources.

The ISO 27002 document covers fourteen major areas:

Information security policies

This section covers the need for an overall security policy as well as the organization and implementation of a cybersecurity plan

Organization of information security

This covers how the security organization is structured within the overall structure and organization of a company. Control and segregation of duties are covered here. It also defines how information on security issues is communicated and working with outside resources and authorities.

Human resource security

Covers risks in hiring as well as ongoing education of employees. It also covers the issues around termination of employment.

Asset management

Lays out how to appropriately manage security assets. This includes acceptable use, issuance, return and labeling. Handling of media and backup information is also covered here.

Access control

User management including control of access to software and hardware within an organization that includes user rights, and restrictions for specific user roles. Service provider access and management is covered here. This also includes password management.

CRYPTOGRAPHY

Covers all aspects of the type of encryption, where it will be used, and how it will be applied within an organization. This also includes advice on management of encryption keys for both active and back up data.

PHYSICAL AND ENVIRONMENTAL SECURITY

This section covers all of the security for facilities used within the organization, including offices and rooms as well as company equipment used outside of the facility.

OPERATIONS SECURITY

This covers all operational activities including the processing and handling of information and communications. Installation and configuration of systems, equipment maintenance and handling including back-up routines, and batch jobs, start up and shut down of systems.

COMMUNICATIONS SECURITY

This covers the protection and management of all networks, segregation of servers and data. Approved electronic messaging, as well as Wi-Fi both in the office and at home are also addressed.

SYSTEM ACQUISITION, DEVELOPMENT AND MAINTENANCE

This includes all hardware used within an organization as well as its management and phase out. This also includes approved software applications and their change control. System acceptance testing is also included.

SUPPLIER RELATIONSHIPS

This covers all supplier and contractors and their relationship issues, including access to all company systems and SLA's (Service Level Agreements).

INCIDENT MANAGEMENT

In the event if there is a breach, this covers who is responsible as a point person and communication processes and procedures for internal as well as external contacts. If there are any regulations for informing authorities it will be covered here. Collection and preservation of evidence is also important and are covered here.

BUSINESS CONTINUITY MANAGEMENT

Information systems are an important part of overall business continuity strategy and plans and they are covered here.

Compliance

Compliance with any legal and contractual requirements are contained in this section. Privacy guidelines and legal implications, ongoing training and education of the workforce as well as record retention and management is covered here.

3. Where to Start

Putting together a comprehensive cybersecurity program can be daunting, particularly for a small business. However, if you start with a simple plan that addresses major risks and then take a series of small steps towards a more comprehensive plan, the process is much less intimidating. So, let’s break down the process of identifying the framework and most important elements of a basic cyber security plan.

The single most important element of your plan is to have buy-in from your employees. Without commitment to implement and follow a proposed plan you are doomed to failure. Next you need to ensure the basics in controlling access. This includes systems and controls to protect your perimeter, both physical and digital, so that only authorized persons are allowed inside. Access points at the perimeter include firewalls, routers, switches, communication lines, Wi-Fi, the hardware and software that control them, and should require rules for setting up and using logins and passwords that allow employees and contractors to gain access into your IT systems.

Next you need to set up basic processes and solutions to protect your data both “at-rest” and “in-transit” in the case your data is exposed. This should include encrypting local storage and cloud storage as well as email and other forms of data in-transit. Good backup practices are essential.

Once you have systems in place you need to make sure your hardware and software remains updated so you continue to protect yourself from the evolving threats to your security.

Hackers can get into your systems through two main paths, either through access points used by employees, customers and contractors, or through malware. An ever evolving threat is “ransomware” which encrypts all your data, in which case you have to either roll back your data to a previous backup or pay the perpetrators a ransom (using Bitcoins, no less) to unlock it.

Finally as we become more interconnected via the Internet you need to be aware of potential new threats that may develop when you connect devices that are not normally thought of as connected to your IT systems, such as security cameras, thermostats, even refrigerators. Which is why we now have a new term call the Internet of Things (IoT)

Any plan without ongoing management and monitoring will also fail so it is important to inspect and follow up any plan you develop.

Let’s get started with the basics.

4. YOUR PLAN

GET BUY-IN FROM YOUR EMPLOYEES

Buy-in from employees goes beyond them just reviewing a document that details company policies for cybersecurity and signing to say they will comply. The key to getting real buy-in is education. Employees should develop an understanding of the need for cybersecurity and the risks to the company and their employment if the organization suffers a breach or “leaks” information. They have to become part of the solution and be involved in ongoing monitoring.

Crucially important in get staff buy-in is follow up and communication from management. Regular meetings between management and staff should be established to discuss what is, or is not, working with your cybersecurity plan.

It’s important to note that the more rigorous your cybersecurity plan is, the greater the communication and buy-in has to be. The reason for this is that an extremely tight security plan may impact normal business workflow and without staff understanding and commitment to the plan employees will start finding ways around the procedures so they can get their work done as easily as possible, which will short-circuit your cybersecurity objectives. Your plan has to balance the needs of your staff to get their jobs done efficiently, while at the same time protecting your data against the broadest spectrum of threats.

Enforcement of a cybersecurity policy is another tricky area that can have both positive and negative effects. Consequences might range from mandatory education for staff members who ignore security policies, to corrective action, or in extreme cases dismissal. The bottom line is that having consequences, even minor ones, is not optional because without them, your plan will not be followed. On the other hand, if the consequences are too harsh, staff morale will suffer and productivity will decrease. In Appendix 1 we’ve included a sample employee technology security policy as a starting point.

SECURING THE PERIMETER AND INTERNAL SYSTEMS

Your perimeter and internal systems management should include reviews of the following:

- Inventory of approved devices and software
- Configurations of mobile devices, laptops, workstations, and servers
- Allocation of administrative privileges
- Maintenance, monitoring, and analysis of audit logs
- Application of email encryption
- Web browser protections
- Malware defenses
- Configurations of network devices such as firewalls, routers, and switches
- User access control based on “need to know”
- Wi-Fi access control

- Internet and external account monitoring and control
- Application software security

The goal of these reviews, which should occur at least quarterly, is to spot deviations from set standards and identify rogue software and hardware.

PASSWORDS

Passwords are a critical component of information security and serve to protect user accounts. The problem is that poorly constructed passwords may result in the compromise of individual user accounts and with that expose the organization's network, resources, and data. Here is an example of a best practice for the creation of strong passwords that could be used in a cybersecurity policy.

Model Password Policy

This policy applies to employees, contractors, consultants, and temporary and other workers, including all personnel affiliated with third parties and applies to all passwords including, but not limited to, user-level accounts, system-level accounts, web accounts, e-mail accounts, screen saver protection, voicemail, and local router and other device logins.

Passwords must meet or exceed the following specifications:

- Contain at least 12 characters
- Contain at least one upper and one lower case letter
- Contain at least one number (for example, 0-9)
- Contain at least one special character, for example;

! $ % ^ & * ( ) _ + | ~ - = \ ` { } [ ] : " ; ' < > ? , /

Poor, or weak, passwords have the following characteristics:

- Contain less than eight characters
- Can be found in a dictionary, including foreign languages, or exist in a language slang, dialect, or jargon
- Contain personal information such as birthdates, addresses, phone numbers, or names of family members, pets, friends, and fantasy characters
- Contain work-related information such as building names, system commands, sites, companies, hardware, or software
- Contain number patterns such as aaabbb, qwerty, zyxwvuts, or 123321
- Contain common words spelled backward, or preceded or followed by a number (for example, terces, secret1 or 1secret)
- Are some version of Welcome123, Password123 or Changeme123"

You must never write down a password. Instead, create passwords that you can remember easily. One way to do this is create a password based on a song title, affirmation, or other phrase. For example, the initial letters phrase, "This May Be One Way To Remember How To Create Passwords" could become the password TmB1w2RH2cp! or another variation.

Note: Do not use any of these examples as a password!

A password manager can be used to both create and manage passwords but must be approved by management in advance.

Policy Compliance

The company cybersecurity team will verify compliance with this policy through various methods, including but not limited to, periodic walk-throughs, video monitoring, business tool reports, internal and external audits, and feedback to the policy owner.

Exceptions

Management must approve any exception to the policy in advance.

Non-Compliance

An employee found to have violated this policy might be subject to disciplinary action, up to and including termination of employment.

Encryption

In any organization, and most particularly in the financial world, the need for confidentiality is central to maintaining the trust of your clients and minimizing the risk of litigation. If a PC is stolen from your office or a laptop is left in the back of a taxi and client data is on the hard drive, the risk of unencrypted data being exposed are real and potentially significant. Thus a policy for the use of encryption in your organization is not just a nice thing to have, it could be the difference between being in business and, quite possibly, going to jail. The following assumes that the company in question is a Microsoft Windows shop; the policies for an Apple OS X shop are similar.

Model Encryption Policy

This policy applies to storage resources used by employees, contractors, consultants, and temporary and other workers, including all personnel affiliated with third parties who store, even temporarily, data files that are the property of the company or the company's clients or affiliates.

Local storage

All desktop PCs and laptops must run Microsoft Windows 8 or above and must be encrypted using Microsoft's BitLocker disk drive encryption.

http://windows.microsoft.com/en-us/windows-vista/bitlocker-drive-encryption-overview

Additional information for installation and use, its advantages and disadvantages, as well as what it protects against is available here:

https://theintercept.com/2015/04/27/encrypting-laptop-like-mean/

Cloud storage

All confidential data stored with a cloud service provider must be encrypted using the native encryption within MS Office or using software such as docNCRYPT or Boxcryptor or other applications that allow the user to manage the encryption keys.

docNCRYPT product link: http://goo.gl/v4WG3L

Boxcryptor product link: https://www.boxcryptor.com/en

Email

All confidential email should be encrypted using email encryption software which encrypts the content of the email message body as well as the attachments. Care should be taken to choose email encryption software that seamlessly fits into the user's workflow and encourages high adoption by both the sender as well as the recipient (such as docNCRYPT for Microsoft Outlook Plugin).

SUMMARY

These model policies are a starting point to create your own company-specific version. The first step to making these and any other security policies actually work is to secure your network perimeter so the bad guys are kept out as well as locking down internal resources by ensuring that all data storage and documents within the network perimeter as well as on external storage are encrypted. At the same time you should be working on educating and getting buy-in from your employees so that they understand the need for these policies and will actively support them.

Cybersecurity doesn't have to be an all-consuming initiative that interferes with getting business done. That said, it does impose an overhead but you have a choice: Continue with a "business as usual" approach to security and run the risk of what could easily become a catastrophe or accept a small amount of organizational overhead and operational discipline to create a robust, secure business environment. Given the increasingly dangerous security landscape of the 21st Century, it should be an easy decision.

We'd love to get feedback from you on this workbook with any suggestions, additions, or comments. Please email us at support@azstec.com and send us your feedback.

Appendix 1: Model Staff Technology Policy

The example policy below can be adapted for your business. Contact us at support@azstec.com if you would like this in Microsoft Word format.

The purpose of this document is to outline the company's policies regarding the use of technology such as computers, mobile devices, email, and Internet usage. These policies are to protect confidential company and client data, which, in turn, will protect you and the company.

The company reserves the right to monitor your use of company-owned internal and external networking and communications facilities. Note that e-mail messages and other uses of the company's computers are not confidential and you should have no expectation of privacy with regard to your use of the firm's technology. Take the time to read this information and ask for any clarifications. Violation of these policies could subject you to disciplinary action up to and including termination of employment. Please sign and date below to acknowledge that you have read and understood this document.

Signed: ________________________________ Date: ___________________

Staff Name: _________________________________

1. **Company-owned technology**: Computers, software, servers, storage devices, the email system and Internet access are owned by the firm and are to be used for company business only. Occasional and brief personal use is permitted as long as it does not interfere with your work. Checking personal webmail using the company's technology is not allowed due to the high risk of viruses.

2. **Company-owned data**: All data including company documents, client records, customer information, and vendor information (wherever stored) belongs to the company and should be treated as confidential and must not be shared with unauthorized parties, including company staff not authorized to view this information. If you are unsure, ask your supervisor.

3. **Employee-owned devices**:
    a. Smartphones: You may use your smartphone to receive and send company email, provided you do the following:

        i. You must employ a device login (password or biometric) and leave the smartphone's auto-lock feature turned on at all times so that your device will turn off automatically after no more than 10 minutes of inactivity.

ii. Use a smartphone that employs encryption of stored data; for example, Apple iPhone, Apple iPad, and Android devices with encryption enabled as well as Microsoft with Exchange Active Sync.
iii. Keep your smartphone's operating system updated.
iv. Remove data from devices you no longer use and wipe them before disposal.
v. Report lost or stolen devices to management to determine if any further action may be required.

b. PCs, laptops, and tablets: You may use your personal computer to remotely login to your company desktop and the company's network for business purposes provided you use the technology that has been provided by the company (such as VPN, virtual desktops or remote desktop services). You should employ the following practices:

i. You must send and receive company email only from your company desktop after you have remotely logged in, or from a device you own if you are using the company's webmail portal, do not send and receive company email directly from a PC, laptop, or tablet that you own (for example by setting up your company email account on desktop Outlook on your device) without management authorization.
ii. Do not store any company data on any PCs, laptops, or tablets that you own that have not been authorized by management.
iii. Employ anti-virus and malware protection software and keep it turned on and up to date.
iv. Use a complex password (see section 5 below) to secure your personal device logins and keep the auto-lock on your devices turned on.
v. Use a complex password (see section 5 below) for your home Wi-Fi network.
vi. Keep your operating systems updated.
vii. Do not "auto save" any company website login locations in your browser.

4. **Good behavior**: Do not use the company's Internet access and email for gambling or in way that might be disruptive, offensive to others, or harmful to morale, including but not limited to sexually explicit messages, images and cartoons, ethnic slurs, racial comments, off-color jokes, or anything that could be construed as harassment or shows disrespect for others, defames, slanders, or otherwise harms another person or business. You are expected to proof and review all social media posts and email prior to sending.

5. **Password policy**: Use strong passwords with the following:

    a. A minimum of 12 characters.
    b. Use at least one upper case and one lower case letter
    c. Use at least one number
    d. Use at least one symbol character (~, ! , #, $, %, ^, &, *, _, +, -, =, <, >, /,”,;, : , [,], {, }, \, or|)

6. **Email transmissions**: You must review your emails prior to sending for the presence of confidential data. Email messages that include confidential information in the message body or attachments must be sent encrypted using the company-provided email encryption software (docNCRYPT). Keep the encryption reminder feature turned on at all times. Email that includes confidential information and requires encryption must be sent from the company’s network. Do not use your smartphone to send confidential email that requires encryption.

7. **Disaster recovery**: To mitigate the impact of a disaster such as fire, earthquake, flood, etc., ensure the following:

    a. Notify management in the event you change your mobile or home phone number. It is crucial that the company always has your most current contact information.
    b. Keep and update any changes to your supervisor’s mobile number and contact your supervisor as soon as possible after a disaster event.
    c. If you are in possession of any company-owned property (such as laptops, USB flash drives, files, etc.), keep them in a safe and secure location.

APPENDIX 2: CYBERSECURITY CONTROLS CHECKLIST

These following sample cybersecurity checklists are to help you identify the areas in your company that need to have security policies and or procedures created.

PHYSICAL SECURITY	NOTES
Designate restricted areas which require authorized access	
Set up appropriate physical access levels for employees, visitors and contractors	
Require staff to wear ID badges (with / without picture)	
Require visitors to wear ID badges	
Require visitors to be escorted into or out of facilities	
Written procedure to cut off physical and virtual access upon termination of employee or contractor	
Require no laptops or tablets in reception area (desktops only)	
Require auto-lock of computer screens after (5) minutes of idle time	
Cable lock of computers in designated areas	
Paper shredders secured and easily accessible by all employees	
Fire-proof cabinets for sensitive paper documents and electronic archives	

CYBERSECURITY POLICIES & PROCEDURES	NOTES
Data backup	
Software updates	
New software application approval and installation	
Password policy	
Mobile device policy	
Online behavior	
Email encryption	
Device encryption	
Remote access	
Cloud storage and transmission	
Employee-owned device usage (BYOD)	
Employee personal webmail	
Logoff and auto-lock of computers	
Emergency evacuation plan	

CYBERSECURITY POLICIES & PROCEDURES (CONT.)	NOTES
Disaster recovery plan	
Disposal of old hardware and electronic media	
Data retention policy (hard and soft copies)	
Employee training and education regarding cybersecurity policies and procedures	

DISASTER RECOVERY	NOTES
Offsite storage of critical data	
Data retrieval procedure for backups and archives	
Updated contact information for management and employees	
Updated contact information for legal counsel	
Updated contact information for law enforcement and emergency services	
Assignment of tasks and designation of management personnel responsible for emergency or security incidents	

APPENDIX 3: RESOURCES

AICPA GENERALLY ACCEPTED PRIVACY PRINCIPLES [“GAPP”]

The American Institute of Certified Public Accountants has disseminated Generally Accepted Privacy Principles (GAPP) “to assist management in creating an effective privacy program that addresses their privacy obligations, risks, and business opportunities”. Although a bit dated, it is still a useful resource for understanding the obligations of CPAs to protect the privacy of client data.

AICPA GAPP link: http://goo.gl/azti5s

CPA Firm Privacy Checklist: http://goo.gl/gDG4XW

ISO/IEC 27001:2013

ISO/IEC 27002:2013 gives guidelines for organizational information security standards and information security management practices including the selection, implementation and management of controls taking into consideration the organization's information security risk environment(s). It is designed to be used by organizations that intend to select controls within the process of implementing an Information Security Management System based on ISO/IEC 27001, implementing commonly accepted information security controls, and or developing their own information security management guidelines.

ISO contact information: http://goo.gl/jgHX7M

SANS

The SANS Institute was established in 1989 as a cooperative research and education organization. Its programs now reach more than 165,000 security professionals around the world. A range of individuals from auditors and network administrators, to chief information security officers from private corporations and universities share lessons they learn and jointly find solutions to the challenges they face.

SANS is the most trusted and by far the largest source for information security training and security certification in the world. It also develops, maintains, and makes available at no cost, the largest collection of research documents about various aspects of information security, and it operates the Internet's early warning system; the Internet Storm Center.

SANS contact information: https://www.sans.org/

NIST

The Computer Security Resource Center (CSRC) facilitates broad sharing of information security tools and practices, provides a resource for information security standards and guidelines, and identifies key security web resources to support users in industry, government, and academia.

CSRC is the primary gateway for gaining access to NIST computer security publications, standards, and guidelines plus other useful security-related information.

NIST contact information http://csrc.nist.gov/

Azstec Security Blog

The Azstec Blog has articles and information regarding current events and solutions to these problems. There are links to other relevant articles and blogs.

Azstec security blog link: http://articles.azstec.com/

Other Blogs and technical resources

Some of our favorites are:

- Bruce Schneier
- Graham Cluley
- Security Magazine
- Krebs on Security
- SearchSecurity
- Information Week Security

There are many others; all you need to do is search for “security news” or “security blogs” and pick out a few that you like and check them weekly. An few minutes each week of just reading about what’s happening in the security world could save you and your company a lot of money and headaches from a data breach.