**POLICY FOR SECURITY**

 The purpose of this document is to clarify and heighten your understanding of Security, specifically Data Security in your daily activities, whether it is administration, sales or service delivery. With the heightened cyber security awareness throughout the world, it is expected that everything we do is inherently secure. Our clients don’t ask, they just expect.

There are no excuses, nor room for assumptions when it comes to securing \_\_\_\_\_\_\_\_\_\_ and our clients’ businesses. With this in mind, it is the responsibility of every \_\_\_\_\_\_\_\_\_\_\_\_\_\_ employee to use good practices when dealing with information, whether electronic or physical.

Our goal is to design, build and continuously refine what is needed to deliver secure solutions to clients and our own business. It is important that we consider and follow these guidelines:

1. All employees are required to take the approved Security Awareness Training no less than annually or as required.
2. Pay attention to people you work with and around.
3. Get to know them and maintain contact.
4. Watch for any unusual activity in and around the business.
5. Hackers can recruit employees to steal data or gain access to data.
6. All Visitors require an escort beyond the main lobby.

### Do not allow a visitor into the office unless you are their escort. They must remain in the lobby until it is confirmed they are expected. They are to be escorted at all times.

### The only exception will be authorized contractors.

### All visitors will be required to have a Visitor badge displayed at all times.

### All contractors will be required to have their appropriate Contractor badge displayed at all times.

###  7. Be very careful and mindful of email attachments and web links

### Do not click on a link or open an email attachment that you were not expecting. Ask questions like “do you know the sender?”, “are you expecting the email?”, “does the attachment make sense?” (i.e.: you are a tech and are receiving an invoice attachment). If in doubt, contact the sender and ask if they sent the email in question.

### Rather than clicking on a web link sent to you, open the browser and type in the URL. Embedded links may not be what they appear to be. Only do this if link meets the previous criteria that you are expecting the link.

 Delete emails that are suspicious without opening the attachments or

 accessing the web link.

## Always use separate personal and business computers, mobile devices and accounts. Do not conduct any business on personal devices.

### Have separate devices for your personal activities including email accounts for personal and business.

### Do NOT conduct business activities from a personal computer that other people (i.e. family) have access. That usage is not in your control in this situation. See Remote Access Policy for details on acceptable remote access guidelines.

### Do NOT use a business computer for personal activities such as shopping, browsing, or gaming where downloads could be compromising.

### Do NOT connect a personal computing device to the company network.

### Do NOT connect a client’s computing device to the company network. Use the appropriate client remediation network for this connectivity as designated by the IT Department.

## Do NOT connect personal or untrusted storage devices or hardware into your computer, mobile device or network.

### Do NOT share USB drives or external storage devices between personal and business computers.

### Do NOT connect or use ANY found USB storage device. (i.e.: USB stick laying in the parking lot).

## DO NOT download and install software. Software installation is restricted. The IT department MUST approve and install any software.

### Do NOT download software from unknown web pages.

### Download software ONLY from the original publisher’s site if approved by IT Department.

### Be very careful of freeware or shareware. Many of these packages have been “re-released” by hackers where they’ve added malware to the original file.

## Do not give out personal or business information.

### Social engineering is an attempt to obtain physical or electronic access to your information by manipulating people. A very common attack involves a person, website or email that pretends to be something it’s not.

### NEVER give out your username or password. No legitimate company would ever ask this. Change your passwords as required by Company policy.

## Watch for harmful popups.

### Popups stating your computer is virus infected and asks you to call or click to clean your computer, or some other unwanted surprising popup are designed to get you to click on the window. Do NOT try to close the window by clicking the X in the upper right corner, the Okay button, or any other button. They are tricking you into clicking on the window to possibly download malware by your action of clicking.

#### If you experience this type of popup, CALL the IT Department immediately.

## Use Strong Passwords.

### Good passwords consist of random numbers, letters and special characters. Good practice is a password length of at least 9 characters, 12 or more is preferred.

### Do not base your password on dictionary words, special dates like birthdays or anniversaries, child or pet names, etcetera. This data is typically found in social media outlets and other easily accessible sources.

### Use a pass phrase such as a sentence you remember then you pull a character from each of the words. You can then change certain characters for some other special character or number and add other special characters such as punctuation into the character string.

### You can also use a password manager that will generate very strong passwords and allow you to access them using one master password. Check the Approved Software listing for approved password managers.

### Two Factor Authentication (2fa) is required for access to network resources.

### Do NOT disable any company installed software or management agents.

### If you feel you have a conflict with installed software, contact the IT Department for remediation.

### Never use priviliged accounts for daily activities.

### Administrator, Privileged, including local admin accounts must only be used to peform as specific function were elevated access is required.

### Handling of Confidential Data.

### Any data generated by the company, for the company, prospects or clients, as well as any data related to prospects, clients, or employees is confidential and property of the company.

### Care should be taken to maintain control and privacy of this confidential information at all times.

### Only use approved storage platforms for this data. Check the Approved Software listing for approved storage platforms.

### Do NOT leave confidential data lying in the open in your work area. See Clean Desk policy for details.

### Confidential Data should be destroyed by shredding, incineration, or recycled using a company approved recycler. Use designated recycling bins at all times.

## What to do if you think you have a problem?

### STOP.

### Contact the IT Department IMMEDIATELY at Extension \_\_\_\_\_ (Helpdesk Number). They will assist you through this incident.

### Not notifying the IT Department could allow any malware to continue to spread and increase the risk to the company.

### Your fast action is the best way to stop this incident in the shortest timeframe.

# Additional Security Policies

Contractor Security Policy

Remote Access Policy

Clean Desk Policy

Incident Response Policy

Approved Software list

Approved Storage Platform list

Company provided hardware assignment document

Mobile device policy

# Security Policy Acceptance

# Name:\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Date: \_\_\_\_\_\_\_\_\_\_\_\_

# Signature line by Employee stating they have read, understand and will comply.

Failure to follow and comply with these guidelines may result in disciplinary action.