ACT SMART I.T.
Helping You Benefit From Today's Technologies

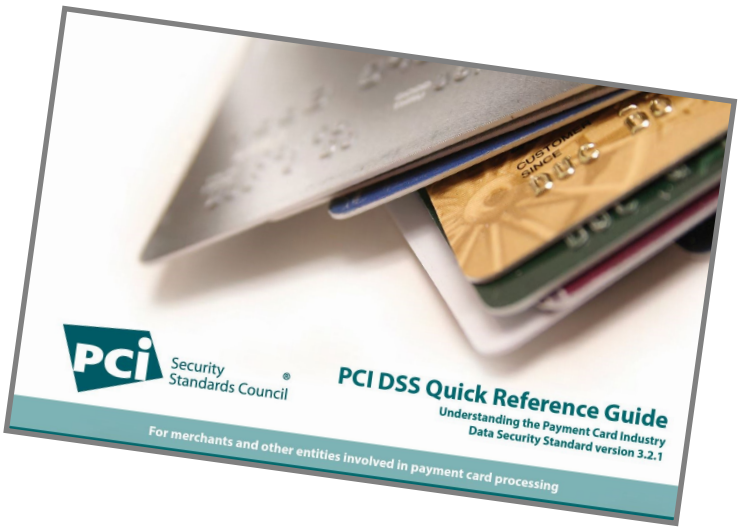
May 2023 BUSINESS EDITION

Don't "Cheat" On This Compliance Document!

(The Self-Assessment Questionnaire from Your Credit Card Company)

Did you just "Check the Box"?
Regulations around security, PCI-DSS compliance and HIPAA are always changing, and the questions are getting more involved and targeted.

I'm finding that many business owners aren't aware of the changes that are taking place. Every time you renew your PCI-DDS compliance and fill out the self-assessment questionnaire, care needs to be exercised. The penalties for non-compliance could put you out of business



WHAT HAPPENS IF YOU VIOLATE PCI COMPLIANCE?
Non-compliance can lead to many different consequences such as monthly penalties, data breaches, legal action, damaged reputation, and even revenue loss. PCI Non-Compliance can result in penalties ranging from $5,000 to $100,000 per month by the Credit Card Companies (Visa, MasterCard, Discover, AMEX)

WHAT IS PCI COMPLIANCE?
Payment card industry (PCI) compliance is mandated by credit card companies to help ensure the security of credit card transactions in the payments industry. Payment card industry compliance refers to the technical and operational standards that businesses follow to secure and protect credit card data provided by cardholders and transmitted through card processing transactions. PCI standards for compliance are developed and managed by the PCI Security Standards Council.

THE 12 REQUIREMENTS OF PCI DSS
The requirements set forth by the PCI SSC are both operational and technical, and the core focus of these rules is always to protect cardholder data.

1. Install and maintain a firewall configuration to protect cardholder data
2. Do not use vendor-supplied defaults for system passwords and other security parameters
3. Protect stored cardholder data
4. Encrypt transmission of cardholder data across open, public networks
5. Use and regularly update anti-virus software or programs
6. Develop and maintain secure systems and applications
7. Restrict access to cardholder data by business need to know
8. Assign a unique ID to each person with computer access

Continued on page 3

Hello Everyone!

I had to write the front page article "Did you just check the box?" because I have talked to several clients recently, who wanted to do just that. Take their chances and misrepresent their compliance with their PCI regulations.

I must stress how risky this can be. If you have an incident where your business is compromised, your insurance most likely will not cover the breach. And, your credit card processing company will most likely issue fines as well as deny your ability to take credit cards due to your fraudulent self-assessment.

We know how hard it is because we are following the same rules, often even more stringent than the ones that apply to you.

Many clients are required to have a penetration test, colloquially known as a "pentest" or ethical hacking, which is an authorized simulated cyberattack on a computer system, performed to evaluate the security of the system. The test is performed to identify weaknesses (also referred to as vulnerabilities), including the potential for unauthorized parties to gain access to the system's features and data, as well as strengths, enabling a full risk assessment to be completed. (Thanks, Wikipedia, for help in that definition!)

After we've had the client's network tested by a third-party service, I review the findings with the business owner or practice manager. As regulations get even stricter, the list of vulnerabilities has also risen. We offer help and guidance to rmitigate these exposures.

If your business requires pentesting, feel free to give me a call. I can walk you through the process and offer you my best recommendations.

At your service,

9. Restrict physical access to cardholder data
10. Track and monitor all access to network resources and cardholder data
11. Regularly test security systems and processes*
12. Maintain a policy that addresses information security for all personnel

***Section #11** has very specific testing requirements and states that you must execute and pass an annual external penetration test as well as quarterly internal security and vulnerability scans. This scanning frequency will change to quarterly for both internal and external scans effective March 31, 2025 under PCI-DDS 4.0

Why PCI DDS 4.0 should be on your Radar?
With the release of PCI v4.0, the countdown has started for organizations already PCO DDS Certified ti transition from PCI DDS v3.2.1 to the new PCI DDS v4.0 standard. Within the timelines of one year to prepare for v4.0 and two years to fully ready for v4.0 future dated requirements, it is time to assess readiness for PCI DDS v4.0 and establish a detailed plan to meet the requirements and timelines.

If you need help with completing your annual self-assessment questionnaire please reach out to me via email david@actsmartit.com or give me a call 781-826-9665. ACTSmart IT is aligned with 3rd party vendors to assist you with meeting today's standards as well as preparing for the upcoming v4.0 changes.

Resource:

PCI DSS Quick Reference Guide (**P**ayment **C**ard **I**ndustry **D**ata **S**ecurity **S**tandard)
For merchants and other entities involved in payment card processing

https://www.pcisecuritystandards.org/pdfs/pci_ssc_quick_guide.pdf

Second of 4 Retention Programs to Launch

Stay interviews are conducted in person, and are essentially, one-on-one interviews in a private setting. A survey tool should be used which details the questions each employee is asked.

You want to come out of the stay interviews with:

- a good understanding of how employees feel about working for the company
- areas of concern which the company may or may not already know about

In my experience, unresolved day-to-day workplace concerns tend to surface, which you want to address prior to an employee launching a job search because they can't resolve their issues.

To give you a better understanding of the value of stay interviews, I can share a recent example of a workplace concern I encountered recently. This workplace concern led him to start passively looking for another job. The employee was frustrated with the communication methods at the company such that he couldn't get answers to his questions in a timely fashion. Because of this, he was unable to complete his projects as quickly as he knew he could. Even though his supervisor did not have a problem with the pace of his work output, he did. At this company, the communication style was entirely done though Zoom or email. The only time leadership would interact in person with employees, was upon hire or termination. This troubled the employee. Learning about his concern gives us the opportunity to "course correct" and alter the communication method. This employee happened to be a top performer as well.

Once you identify areas of concern, you can develop your HR initiatives to focus on making improvements to those areas of concern for the coming year. One of the key questions on the stay interview is, "Why do you stay?". We are not only interested in why people left. Whatever reasons employees have for remaining with your company we need to not only do more of, but publicly promote. This information is critical.

Once you conduct stay interviews annually, you can compare differences in employee sentiment from year to year, which may be impacted by changes in the workplace environment, leadership, business direction, or the economy.

The information gleaned from these stay interviews has proven to be extraordinarily valuable with my clients. The value stay interviews could provide includes improvements to process, procedures, and even the design of a position, pay, benefits, schedules, workflow, etc. The program pays for itself if we prevent the loss of our valued employees.

I would rather a client implement the stay interview program before implementing an exit interview program, as I want the information before a loss which I can potentially do something about. Information gleaned at the time of the exit interview is just too late.

The very last question that I ask when conducting stay interviews is to ask each employee for the name of someone who might be interested in joining our team if we followed up with them. I found that the majority of employees will supply a name and contact information of a potential new employee. Many employees know of potential employees, but not many employees refer others unless there is either something in it for them, or someone asks them directly for a referral. If every supervisor sat down with their employees individually and asked for a name, you would have a list of potential recruits. Stay interviews can be conducted by a third party or by HR staff. There are advantages and disadvantages to both.

*Note from the Editor: Somehow we strayed from Debra's **4 Retention Programs to Launch** last month. We're back on track with her second program. If you missed the first program in our March issue, check out our newsletter archives.*

in 2023; Stay Interviews

For instance, sometimes employees won't share their true feelings with a member of company management, even HR, as they may not been seen as objective, or employee focused. But, using a consultant can sometimes be a challenge if they don't understand your business and company dynamics. This can be disadvantage can be overcome, however, by proper preparation prior to the survey.

Conducting stay interviews gives you data; data to inform your people decisions. It is a low-cost initiative with countless benefits. I would rather know what is on the minds of my employees while they are still working for me, than having to find out what was on their minds from an exit interview.

Debra J. Parent, PHR, SHRM-CP, CHHR
rightfitrecruiting@comcast.net,
(508) 884-6798
https://rightfitrecruitingservices.com/
Or connect with Deb via LinkedIn –
https://www.linkedin.com/company/djp-right-fit-recruiting-llc/about/

You can view Debra's recent webinars at:
https://actsmartit.com/recruit

How To Stay Safe on Social Media

Our social media apps are part of our lives and like any convenient tool (think email, your smart phone and car) they need to be managed and mastered. Every day brings new challenges to your safety and security. Here are some of the ways to keep yourself protected and secure:

Treat your personal info like cash and think hard before you give it away.

Check your settings. Even if the social media app isn't asking you for data, assume that it is collecting it with your implied acceptance. Mark your mobile device settings (Camera, Microphone, Location, Sync contacts) to OFF until they are needed for that function and then reset the default to OFF.

Enable MFA (Multi-factor authentication also known as 2 factor authentication. It makes it hard for hackers to access your online accounts, even if they know your passwords.

Use long, strong and unique passwords. (See ACTSmartIT.com/passwords for our guide)

Share with Care! The more information that you post, the easier it is for hackers to steal your identity and commit other crimes. Think who you allow to see your personal posts; most platforms allow you to limit who can see or engage with you.

THINK BEFORE YOU POST! Posts stay around forever and may come back to haunt you!

Think twice before accepting a request or invitation to connect from just anyone. Many social media networks have tools that allow you to manage the info you share with friends in different groups.

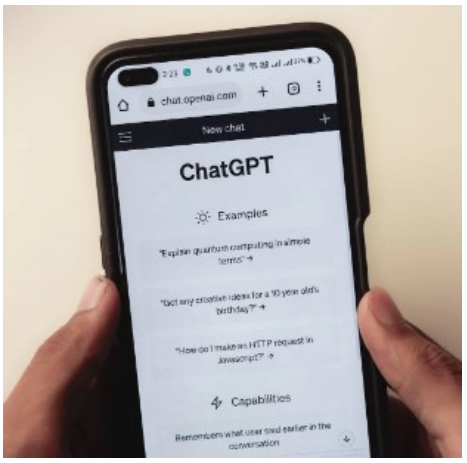
For more information about social media safety including many social media apps and our articles' resources, go to ACTSmartIT.com/social

You can also request a FREE printed Infographic "How To Stay Safe on Social Media which includes tips and the dangers of 5 of the most popular apps.

ACTSmartIT.com/social

We Asked ChatGPT

The top 5 reasons for a small business to issue a press release



Over the years, PR Works has offered many PR Pointers about when you should issue a press release. With the entire world gone AI coo-coo, we thought it might be a good idea to ask ChatGPT what it thought. Here's the answer:

1. **New product or service launch**: A press release can be used to announce the launch of a new product or service. This is a great way to generate buzz and get the word out to potential customers.
2. **Company milestones:** Press releases can be used to announce significant milestones for your small business. This could be opening a new location, a significant sales achievement, or a major partnership or collaboration.
3. **Awards and recognitions:** If your small business has received an award or recognition, a press release can be used to announce the achievement. This can help to build credibility and increase visibility for your business.
4. **Events:** If your small business is hosting an event, a press release can be used to generate interest and encourage attendance. This could be anything from a grand opening to a charity fundraiser.

These four answers aren't exactly groundbreaking. In fact, PR Works routinely recommends this to prospects and clients. The fifth, however, dug a little deeper:

5. **Expert commentary**: If you or someone in your small business has expertise in a particular area, a press release can be used to position your business as a thought leader. This can help to build credibility and increase visibility, leading to new business opportunities.

This response makes a real case for not using AI to draft your press releases or media pitches.

Why?

You can issue a release touting you or your firm's expertise. If you use AI to create that release, you are selling yourself short. Worse, you probably will not create a release that moves the needle enough to get any traction.

That aside, positioning you or your company as the expert takes some nurturing with a combination of releases, follow-up calls, and pitches to targeted media publications and contacts. AI can't do that.

You may strike thunder once in a blue moon and some publication will run a release or reach out in response to a release and ask for your expert opinion—a blind squirrel will occasionally find a nut. You really do need a campaign approach to gaining expert status. Something that live humans like the folks here at PR Works can do for you.

Steve Dubin

If would like assistance in putting together a PR campaign or issuing individuals releases for any of the above, give us a call

PRWorks

18 Main Street Extension, Suite 409
Plymouth, MA 02360
781-582-1061

ACTSmart IT
332 Main Street
Wareham, MA 02571

In This Issue

«First Name» «Last Name»
«Company»
«Address»
«City», «State» «Postal Code»

A Password Manager Can Really Help With Compliance!

Passportal

Take control of your passwords and system access—and get peace of mind

- No more remembering dozens of passwords
- Faster access to websites and applications
- Centralized system for both corporate and personal passwords
- Folders to organize and categorize credentials
- Automatic generation of audits and reports to help with tracking and regulatory compliance reporting
- Save time with instant credential insertion—no more remembering lists of passwords
- Centrally control employee access to systems, so only those who should be on critical systems have access
- Easily terminate access to systems following an employee's departure
- Track and record system access to help meet compliance audit requirements

Go to *ACTSmartIT.com/passportal* for more information and pricing