HAWAII JSOX NEWSLETTER

Apr 2023 Vol. 14

PRESIDENT'S MESSAGE

Knowing the importance of J-SOX compliance, I thank you all for your efforts to remain compliant in your areas despite a very busy 2022. As procedures and processes continue to evolve, please communicate changes and updates with the team to ensure our continued adherence to necessary guidelines. It is imperative that we remain J-SOX compliant, so I appreciate your continued cooperation. Mahalo!

ADMINISTRATION & COMPLIANCE

The results for 2022's JSOX testing were as follows:

ELC – No deficiencies were noted.
PLC – No deficiencies were noted.
FSCP – No deficiencies were noted.
ITGC – No deficiencies were noted.

Upcoming JSOX Testing

ELC Design: Q2-3
(FSCP) ELC Design: Q2-3
PLC Design: Q3-4
FSCP Design: Q3-4
ITGC: Q2

Please keep in mind the importance of the JSOX procedures and guidelines we have in place, including notifying Admin & Compliance of any significant process changes. Thank you!

Special Approval Authority Reminder:

Thank you for your continued cooperation and efforts to maintain JSOX Compliance. I wanted to remind everyone about the Scope of Authority and associated Special Approval Authority requests.

The Scope of Authority (attached) denotes levels of authority based on an employee's position and the associated requirements for processing approvals, particularly for "significant" activities. Please review the Scope of Authority document to ensure that you have a general understanding of the requirements therein. The most recent version can be found in the Workgroup under Everyone > Scope of Authority. Generally speaking, the most applicable tabs for the majority of employees will fall under the General or LLC tabs. For more specific information, please refer to the other tabs relevant to your position (i.e. Marketing/Sales/Planning/HR) if applicable.

Within the Scope of Authority, you will notice that the central five columns contain check marks denoting the level of approval required. If there is a check in the "Special Approval Authority" cell, that indicates that a Special Approval Authority is also required. In completing the Special Approval Authority form you will need to fill out the required information for your submission. All fields are required, with minor differences in the required signatures. It is not expected to have every line signed, only the ones relevant to the request and based on the Scope of Authority.

As a way of tracking these requests, please contact me directly (t.lee@princehawaii.com) for the proposal number PRIOR to submitting the SAA for signature. This ensures that I am able to track all SAAs in motion.

FEEDBACK

Employees can reach Tim Lee at t.lee@*princehawaii.com or (808)944-3286* with comments, concerns and other feedback. Mahalo!

Prince Resorts Hawaii

JSOX COMMITTEE

SHIGEKI YAMANE

JUN KOBAYASHI

TIM LEE

RYAN DOI

HUMAN RESOURCES

The Prince Integrity Hotline is available for you to report ethical concerns, safety or security items, or any other questionable situations with complete anonymity and confidentiality.

PRINCE INTEGRITY HOTLINE:
1 (877) – 774 - 5769

HAWAII JSOX NEWSLETTER

Jan 2022 Vol. 13

INFORMATION TECHNOLOGY

PHISHING ATTACKS ARE GETTING TRICKIER

Phishing attacks have become the most common method cyber attackers use to target people at work and at home. Phishing attacks have traditionally been emails sent by cyber attackers to trick you into doing something you should not do, such as opening an infected email attachment, clicking on a malicious link, or sharing your password. While traditional phishing attacks continue today, many cyber attackers are creating advanced phishing emails that are more customized and harder to detect. They are also using technologies such as text messaging, social media, or even telephone calls to engage and fool you. Here are their latest tricks and how you can spot them.

Cyber Attackers Are Doing Their Research

Phishing emails used to be easier to detect because they were generic messages sent out to millions of random people. Cyber attackers had no idea who would fall victim; they just knew the more emails they sent, the more people they could trick. We could often detect these simpler attacks by looking for odd emails with "Dear Customer" in the beginning, misspellings, or messages that were too good to be true, such as Nigerian princes offering you millions of dollars

Today's cyber attackers are far more sophisticated. They now research their intended victims to create a more customized attack. Instead of sending out a phishing email to five million people, or appearing to be generic emails sent by corporations, they may send it to just five people and tailor the attack to appear to be sent from someone we know. Cyber attackers do this by:

- researching our LinkedIn profiles, what we post on social media, or by using information that is publicly available or found on the Dark Web.
- crafting messages that appear to come from management, coworkers, or vendors you know and work with.
- learning what your hobbies are and sending a message to you pretending to be someone who shares a mutual interest.
- determining you have been to a recent conference or just returned from a trip and then crafting an email referencing your travels.

Cyber attackers are actively using other methods to send the same messages, such as texting you or even calling you directly by phone.

How to Detect These More Advanced Phishing Attacks

Because cyber attackers are taking their time and researching their intended victims, it can be more difficult to spot these attacks. The good news is you can still spot them if you know what you are looking for. Ask yourself the following questions before taking action on a suspicious message:

1. Does the message create a heightened sense of urgency? Are you being pressured to bypass your organization's security policies? Are you being rushed into making a mistake? The greater the pressure or sense of urgency, the more likely this is an attack.
2. Does the email or message make sense? Would the CEO of your company urgently text you asking for help? Does your supervisor really need you to rush out and buy gift cards? Why would your bank or credit card company be asking for personal information they should already have about you? If the message seems odd or out of place, it may be an attack.
3. Are you receiving a work-related email from a trusted coworker or perhaps your supervisor, but the email is using a personal email address such as @gmail.com?
4. Did you receive an email or message from someone you know, but the wording, tone of voice or signature in the message is wrong and unusual?

If a message seems odd or suspicious, it may be an attack. If you want to confirm if an email or message is legitimate, one option is to call the individual or organization sending you the message with a trusted phone number.

You are by far the best defense. Use common sense.