

Information Security Onboarding Addendum – Sub-Vendor

Date

I, CHAITANYA (Print Name), an employee of, SAVVY IT INC ("Sub-Vendor") working through TEKsystems currently assigned to its Customer, hereby acknowledge that I have spoken to the local market TEKsystems Company Representative, _____, ("company representative") regarding the Customer and TEKsystems Information Security Policies. During this discussion, the company representative and I discussed the awareness, importance, and reinforcement of both Customer and TEKsystems Information Security Policies.

As an initial matter, the company representative reminded me that the Customer is monitoring my activities while on assignment through TEKsystems as a an employee of, SAVVY IT INC ("Sub-Vendor") to ensure compliance with the respective Information Security policies.

In that regard, the company representative and I specifically discussed the following:

- The prohibition regarding the downloading or transferring of ANY data or files to an external device or email without, prior, written consent of Customer.
- The prohibition regarding the use of a file sharing service or cloud based service such as GitHub or DropBox or posting any data to any external site.
- The importance of recognizing that any data or information provided to me or to which I have access to or actually access while assigned to Customer is not only intellectual property of Customer but also confidential and proprietary data of Customer (the "Data"), and that at no time shall I disclose the Data.
- The criticality of ensuring that Protected Health Information ("PHI"), Personally Identifiable Information ("PII") or Intellectual Property ("IP") is kept confidential and handled in a manner consistent with Customer standards.
- The requirement to periodically review the Information Security Training provided to me by TEKsystems to ensure Information Security compliance.
- If any request is made of me to deviate from either or both Customers' or TEKsystems' Information Security Policy, that I will immediately contact my company representative.

Additionally, I will take all measures to prevent any of the following actions which could lead to a potential Information Security breach:

- Loss or theft of a Customer or TEKsystems issued device / laptop containing Customer information
- Unauthorized download, transmission, use / access or disclosure of customer information
- Insertion of malicious software on Customer's system
- Any loss or theft of a Customer-provided ID/security badge, key, password token, access credentials or key card

Finally, the company representative and I discussed the additional following measure I will follow:

- Ensure use of only Customer-authorized devices and networks
- Obtain Customer's prior, written authorization before saving ANY information to a portable device (e.g., USB drive, CD, iPod, iPad, mobile phone) and/or removing that device from the Customer premises. Ensure that workstations and authorized portable storage devices are locked at all times when I am away from my work station

Sincerely,

Company Representative: _____

(Signature)

ACKNOWLEDGED:

CHAITANYA SWAROOPA BOYAPATI
(Print Name)

B. Chaitanya
(Signature)