

## Table of Contents

---

1.0	GENERAL .....	2
1.1	SUMMARY .....	2
1.2	REFERENCES .....	2
1.3	SUBMITTALS .....	2
1.3.1	<i>General</i> .....	2
1.3.2	<i>Service Request Criteria</i> .....	3
1.4	EXPECTATIONS .....	3
1.4.1	<i>OTech</i> .....	3
1.4.2	<i>Customer</i> .....	3
1.5	SCHEDULING .....	3
1.5.1	<i>Change Management Schedule</i> .....	4
1.6	DEFINITIONS .....	4
<hr/>		
2.0	PRODUCTS .....	5
2.1	Client Products .....	5
<hr/>		
3.0	EXECUTION .....	6
3.1	SECURITY .....	6
3.2	QUALITY CONTROL .....	6
3.2.1	<i>OTech Responsibilities</i> .....	6
3.2.2	<i>Customer Responsibilities</i> .....	6
3.3	SUPPORT AVAILABILITY .....	6
3.4	INSTALLATION .....	6
3.4.1	<i>OTech Responsibilities</i> .....	6
3.4.2	<i>Customer Responsibilities</i> .....	6

## 1.0 GENERAL

### 1.1 SUMMARY

The Office of Technology Services (OTech) performs server vulnerability scanning within the Application Hosting offering. These scans proactively identify known vulnerabilities of computing systems in the network to determine if and where weaknesses in a system can be exploited and/or threatened. OTech can provide a routine or on-demand report of scan findings to Customers so that potential exploits of their hosted server(s) can be mitigated.

Routine scans are performed on all platforms within Application Hosting however scan reports are only available upon request.

### 1.2 REFERENCES

Items referenced here are found elsewhere in this document.

	IDENTIFIER	DATE	TITLE
	Website		<a href="#">Common Vulnerabilities and Exposures</a>
	Website		<a href="#">Common Vulnerability Scoring System</a>
	3300		Vulnerability Management Policy
	3303		Network Server Vulnerability Scan Procedure

### 1.3 SUBMITTALS

#### 1.3.1 General

Use the following method for work requests:

Item	Request Method
Quotes & Billable Service	<a href="#">OTech Customer Service System (CSS) Request</a>
Modifications to Existing Systems	<a href="#">OTech Service Desk</a> , <a href="#">CSS</a> or <a href="#">Remedy Service Request</a>
Technical Problems	<a href="#">OTech Service Desk</a> or <a href="#">Remedy Incident</a>
Security Related Issues/Incidents	<a href="#">OTech Service Desk</a>

Include the Customer's name, contact information and associated project name on forms, documents, and requests submitted to OTech.

### **1.3.2 Service Request Criteria**

A completed Vulnerability Scan Submittal is required prior to the start of work. To aid in the preparation of providing this technology, all information must be included in the OTech Service Request. [Customer Service System \(CSS\)](#).

This Submittal is to be revised at appropriate intervals providing for expeditious and practicable execution of the Work. Revised submittal(s) must indicate changes, if any.

## **1.4 EXPECTATIONS**

### **1.4.1 OTech**

OTech will conduct the vulnerability scans.

OTech will only provide the scan reports to authorized staff person(s) identified within the Service Request.

OTech maintains copies of scan report only until the subsequent month's scan is run or for 30 days from the scan; whichever arrives first.

OTech follows change management practices. Change requests are recorded in [OTech Remedy Service Request](#) system, as a Change Request (CRQ). Contact your OTech account managers for current change procedures.

### **1.4.2 Customer**

Customers are expected to understand product lifecycles and collaborate with OTech on upgrades, testing, and verification of their platform and software technology should features of the outdated product(s) trigger adverse scan results.

It is expected that Customers will analyze the vulnerability scan results and submit technology modification requests as needed to remediate findings that result from the vulnerability scanning process.

Requested discussion with OTech beyond a clarification of scan reports may result in an additional consulting fee.

## **1.5 SCHEDULING**

Subscriptions to scan reports will be provided monthly.

On-Demand report requests will be scheduled during a time agreed upon by OTech and the Customer.

### 1.5.1 Change Management Schedule

Change proposal / requests follow the established OTech Change Management process. Work performed during scheduled maintenance periods is subject to the OTech Change Management Schedule. Changes require 2-week prior notification. Shorter periods may not always be expedited; additional charges may be incurred for expedited change requests.

## 1.6 DEFINITIONS

<b>Term, phrase, abbreviation</b>	<b>Definition</b>
Vulnerability	A weakness which allows an attacker to reduce a system's information assurance.
CVE	Common Vulnerability Exposures
CVSS	Common Vulnerability Scoring System

## 2.0 PRODUCTS

### 2.1 *Client Products*

Adobe Reader

## **3.0 EXECUTION**

### **3.1 SECURITY**

The Information Security Officer accountable for data contained on the system to be scanned must approve the scan prior to the start of work. Reference the CSS routing process for obtaining approval.

### **3.2 QUALITY CONTROL**

Not used.

#### **3.2.1 OTech Responsibilities**

- Review and approval of submitted information prior to beginning work
- Notify Customer of submittal flaws, if any

#### **3.2.2 Customer Responsibilities**

- Submit complete 1.3 – SUBMITTALS information

### **3.3 SUPPORT AVAILABILITY**

Core business hours for report clarifications are Monday through Friday 0800-1700. State holidays and mandated schedule alterations are observed and may impact staff availability.

## **3.4 INSTALLATION**

#### **3.4.1 OTech Responsibilities**

- Create and maintain scan report generating scripts
- Produce and deliver scan reports to the customer
- Provide brief follow-up report clarifications, if any

#### **3.4.2 Customer Responsibilities**

- Notification of receipt to OTech of scan report
- Review of scan report for completeness
- Charges as a result of excessive scan report discussion