9021 Arboretum Parkway, Suite 140 • Richmond, VA 23236
info@uptechsecurity.com
(804) 213-2562

VULNERABILITY ASSESSMENT REQUIREMENTS

1. PURPOSE

[redacted] must protect controlled, confidential or sensitive data from loss to avoid reputation harm and to avoid unfavorably impacting our clients. Institution of vulnerability assessments will be used to identify vulnerabilities on the [redacted] networked computing devices, inclusive of mobile devices which may access [redacted]. The results of the vulnerability scans help inform management and computing device administrators of known and potential vulnerabilities on so those vulnerabilities can be addressed and managed. Vulnerability scanning can be used at a broader level to ensure that [redacted] are working correctly and are effective.

2. SCOPE

This policy applies to all employees, contractors, subcontractors, temporary and other workers, including all personnel affiliated with third parties who access or utilize information systems owned or are provided by [redacted], or information systems which contain [redacted] assets, or paper copies of any data related to [redacted] Any changes within the [redacted] environment follow the guidelines as [redacted].

2.1. The purpose of scope including contractors and subcontractors is directly related to recent breaches of large commercial and federal institutions [redacted], where the breach was directly related to contractor and subcontractor negligence.

3. STANDARD

3.1. Approved Scanning Tool (Internal)

9021 Arboretum Parkway, Suite 140 • Richmond, VA 23236
info@uptechsecurity.com
(804) 213-2562

3.1.1. While there are numerous tools that can provide insight into system vulnerabilities, not all scanning tools possess the same set of features. [redacted], or their assignee is responsible for approving and overseeing organizational use of vetted scanning and assessment tools for internal network usage. Use of any other vulnerability scanner must be justified [redacted].

3.1.2. No third-party shall have access to confidential or protected information within the [redacted] explicit, written approval from the [redacted].

3.1.2.1. Third-Parties with access to said data must agree to abide by the terms set forth in this document as to vulnerability scanning and mitigation.

3.1.3. Any approved scanning tool must be capable of scanning information systems from a central location and be able to provide remediation suggestions. It must also be able to associate a severity value based on Common Vulnerability Exploits as defined by the National Institute of Standards and Technology National Vulnerability Database to each vulnerability discovered based on the relative impact of the vulnerability to the affected unit.

3.1.3.1. The tool chosen for approved scanning is [redacted]

3.2. Periodic Vulnerability Scanning

3.2.1. [redacted] periodic vulnerability scanning on all networked devices, with the minimum of quarterly scans using the predefined approved scanning tool.

9021 Arboretum Parkway, Suite 140 • Richmond, VA 23236
info@uptechsecurity.com
(804) 213-2562

3.2.2. Monthly internal scans are required for any device which has or has had access to data deemed as restricted, confidential, or could release customer records, including, but not limited to, servers, backups, network infrastructure, virtual machines, and devices that must meet specific regulatory requirements.

3.2.3. Scans will be conducted during hours appropriate to the needs of the business in efforts to minimize disruption to practical business functions.

3.2.4. All data obtained through the scans is to be treated as internal, confidential records.

3.2.5. System and network administrators must not make any temporary changes to networked computing devices for the sole purpose of passing an assessment. Any attempts to tamper with results will be referred to management for potential disciplinary action.

3.2.5.1. No devices connected to the network shall be specifically configured to block vulnerability scans from authorized scanning engines.

3.2.6. Vulnerabilities on networked computing devices shall be mitigated and eliminated through proper analysis and repair methodologies as outlined in the [redacted].

3.3. New Information System Scanning and Hardening

3.3.1. No new information system shall be considered or added to a production environment until a full vulnerability assessment has been conducted and vulnerabilities mitigated.

3.3.2. When available, new information systems shall be validated using [redacted] to

9021 Arboretum Parkway, Suite 140 • Richmond, VA 23236
info@uptechsecurity.com
(804) 213-2562

ensure that hardened security templates are applied to the system before being added to the production environment.

3.3.3. Vulnerability assessments will be conducted on new information systems at the completion of the operating system installation and patching, at the completion [redacted], and at the completion of any vendor provided or in-house developed application.

3.3.4. At the completion of the aforementioned vulnerability assessment and hardening, all discovered vulnerabilities must be documented and remediated. Documents will be stored in a secure cloud-based repository which meets requirements under the [redacted] for future reference.

4. EXTERNAL AUDIT AND TESTING

4.1. External audit of outward facing infrastructure is to be completed on a quarterly basis by a qualified individual or third party. Said audit would consist of standard vulnerability assessment, and may involve the use of tools outside the scope of the approved scanning tool with the condition of the reporting outlining vulnerabilities and associating a severity value based on Common Vulnerability Exploits as defined by the National Institute of Standards and Technology National Vulnerability Database to each vulnerability discovered based on the relative impact of the vulnerability to the affected unit.

4.2. An annualized in-depth Penetration Test is to be conducted on all outward facing infrastructure, to ensure there were no

undetected vulnerabilities. Said test is to be conducted by a certified security professional to be validated as to qualification, certification, and background [redacted].

4.3. Findings from external audits or penetration testing are to be mitigated in a prompt fashion.

4.3.1. Vulnerability findings are to be documented and retained in a secure cloud-based repository which meets requirements under the [redacted].

5. USE OF OUTSIDE CONTRACTORS

5.1. [redacted] at its discretion utilize outside contractors to complete the required work, however, the tools used must, at minimum meet or exceed the capabilities of the approved tool.

5.1.1. Many tools utilized by outside contractors are not within the scope of this document due to variation, however, the final report must meet or exceed requirements set forth in section *3.1.3*.

5.2. Any and all outside contractors must sign a formal non-disclosure agreement before work begins or before scope of work is discussed.

5.2.1. Validated digital signatures are considered acceptable as signatory methods.

9021 Arboretum Parkway, Suite 140 • Richmond, VA 23236
info@uptechsecurity.com
(804) 213-2562

5.2.1.1. Guidance on digital signatures is outlined directly in the eSign Act of 2000, codified as the Code of Federal Regulations Title 12 § 609.910, and Title 15 § 609.910.

5.3. Any and all outside contractors must be properly vetted by [redacted] their background and ability to properly perform testing.

5.3.1. Information as to proper vetting procedures can be found within the [redacted].

6. EXCEPTIONS

There are no exceptions accepted to this section unless pre-approved and justified [redacted].

7. NON-COMPLIANCE

An employee, contactor, or subcontractor found to have violated these standards may be subject to disciplinary action, up to and including termination of employment. Additional ramifications such as civil or criminal prosecution may apply depending upon the severity of the violation.

8. CONTACTS

If you have any questions or concerns regarding this policy, or would like to report a policy violation, or lack of proper scanning, or have scanning results that show a vulnerability, [redacted].