Vulnerability Assessment Procedure

Jadarah For Dept Collections Co.

This document is a property of **Jadarah For Dept Collections Co.** and contains sensitive and confidential information which should not be disclosed, transmitted, duplicated, and used in whole or part other than for its intended purpose and recipients

Document Control Information

Document Version Control Information				
Version	Date	Author	Reviewer	Approver
1.0	**03 Oct 2024**	Abdulrahman AlJamani	Ahmed Al-Kelani	Misfer Al-Ajmi

Document Change History Information			
Author	Date	Version	Change Description

Contents

Document Control Information **2**

1 Introduction **4**

2 User registration **5**

2.1 Scope Definition 5

2.2 Prerequisite 5

2.3 Timing and scheduling 5

2.4 Procedure steps 5

2.5 Auditing and logging 6

2.6 Monitoring 6

1 Introduction

This document sets out a procedure to be used to assess technical vulnerabilities within the IT environment. Its intended audience is IT and information security management and support staff who will implement and maintain the organization's defences.

This procedure is intended to be used by a suitably qualified specialist with a specific brief to assess a defined scope of systems and networks. It must only be used where the written permission of the owner of the systems and networks to be assessed has been obtained. If there is any doubt about this, the procedure should not be performed, and clarification should be sought.

This control applies to all systems, people and processes that constitute the organization's information systems, including board members, directors, employees, suppliers and other third parties who have access to Jadarah For Dept Collections Co. systems.

The following policies and procedures are relevant to this document:

- *Change Management Process*
- *Software Policy*
- *Anti-Malware Policy*
- *Technical Vulnerability Management Policy*

2 User registration

WARNING: This procedure is intended to be used by a suitably qualified specialist with a specific brief to assess a defined scope of systems and networks. It must only be used where the written permission of the owner of the systems and networks to be assessed has been obtained. If there is any doubt about this, the procedure should not be performed, and clarification should be sought.

The vulnerability assessment will be carried out as and outsourced service by qualified and experienced specialists at the specific request of senior management and is subject to full security protection (e.g., anti-virus, firewall) as per Jadarah For Dept Collections Co. policies. Detail regarding how to use these tools is not provided in this procedure.

2.1 Scope Definition

The scope of the vulnerability assessment should be documented in as much detail as possible. According to the areas covered, this detail should include as a minimum:

- External assessment
  - External IP addresses included
  - External IP addresses specifically excluded
  - Websites included
- Internal Assessment
  - Names of servers included
  - IP address ranges included
  - IP addresses specifically excluded
  - User computers to be assessed

The agreed scope should be signed off by Chief Information Security Officer (CISO) and IT Manager.

2.2 Prerequisite

Before starting the assessment, the following prerequisites must be in place:

- The assessment scope is fully defined
- Written permission is provided for the defined scope
- Assessors are adequately trained on the tools to be used and the vulnerability assessment process
- Service managers of the systems to be assessed have been informed of the purpose and timing of the exercise
- The tools to be used are installed and fully updated

2.3 Timing and scheduling

In general, it is desirable to run the scanning aspects of this procedure out of normal business hours although this may be relaxed with the prior agreement of management.

2.4 Procedure steps

The delegated representative from Jadarah For Dept Collections Co. should ensure that at minimum the vulnerability assessment should consist of the following steps:

1. Reconnaissance
2. External Scanning
3. Internal Scanning
4. Reporting

Once the initial reconnaissance stage has been completed scanning for vulnerabilities can be carried out. This will be in two stages:

1. External scanning of the network perimeter from outside the organization network
2. Internal scanning of specific networks, servers and clients from within the network perimeter

Both types of scans are required in order to assess vulnerabilities from external and internal threats. A full report will then be produced.

2.5 Auditing and logging

All the records should be kept of all activities carried out as part of the vulnerability assessment, including names, dates and times under the custody of Jadarah For Dept Collections Co..

2.6 Monitoring

All scans should be monitored in real time. Scans should not be left to run unattended overnight or over a weekend or scheduled at such times.