Vulnerability Management Policy

v1.0

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 Technical Vulnerability Management Policy **4**

2.1 What is a technical vulnerability? 4

2.2 Sources of Information 4

2.3 Patches and updates 5

2.4 Vulnerability assessment 6

2.5 Hardening 6

2.6 Awareness training 6

1 Introduction

It is essential that effective precautions are taken by Jadarah For Dept Collections Co. to protect itself against this threat which can come from a number of sources including organised gangs, competitor organizations, politically motivated groups, rogue employees, nation state sponsored “cyber-warfare” units or simply individuals exercising curiosity or testing their skills.

Whatever the source, the result of a successful security breach is that the organization and its stakeholders are affected, sometimes seriously, and harm is caused.

Malware comes in many forms and is constantly changing as previous attack routes are closed and new ones are found. For malicious software to carry out its intended purpose it needs to be installed on the target device or computer. There are a number of key ways in which malware infects computers and networks, although new ways are being created all the time.

The most common infection techniques are as follows.

- Phishing
- Websites and Mobile Code
- Removable Media
- Hacking

But for these techniques to be used by an attacker, they must take advantage of a vulnerability in our defences.

This document sets out the organization’s policy on how it will assess and manage technical vulnerabilities within the IT environment, which includes the cloud services it uses. Its intended audience is IT and information security management and support staff who will implement and maintain the organization’s defences.

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.’s systems.

2 Technical Vulnerability Management Policy

2.1 What is a technical vulnerability?

A vulnerability is commonly defined as “an inherent weakness in an information system, security procedures, internal controls, or implementation that could be exploited by a threat source.”

These vulnerabilities are constantly being found and corrected via software updates or patches. Unfortunately, it is not always the developer or user who discovers these vulnerabilities. When discovered by a potential attacker the vulnerability becomes something to be exploited for gain and kept secret for as long as possible. A newly discovered vulnerability is often referred to as a “zero-day exploit” and is difficult to defend against.

Jadarah For Dept Collections Co.’s policy with respect to technical vulnerabilities is to be aware of them and to close them where possible, either directly or via other means.

2.2 Sources of Information

The first step in managing technical vulnerabilities is to become aware of them. Since we are talking about technical vulnerabilities these will of course depend upon the technology employed within the organization. It is necessary then to gain a full appreciation of the technology components that make

up the organization's infrastructure and their versions (since most technical vulnerabilities are very version-specific).

This should include:

- Operating systems e.g. Windows, UNIX, Cisco
- Databases e.g. SQL Server, MySQL
- Web servers e.g. IIS, Apache
- Desktop software e.g. Office, Acrobat
- Web technologies e.g. Flash, Java
- Application software e.g. SAP, Agresso
- Hardware e.g. servers, routers

Information about vulnerabilities with any of the above components is generally available from the vendor who will issue updates and patches to fix those that it becomes aware of.

A process must therefore be put in place to ensure that all relevant information about updates is being received and reviewed by competent staff members. This will usually give guidance about the level of urgency associated with each update.

Where configuration changes are recommended to close off vulnerabilities, these must be actioned through the organization change management process so that appropriate controls are in place for testing, risks assessment and backout.

For cloud services, the responsibilities of the cloud service provider (CSP) and Jadarah For Dept Collections Co. as the cloud service customer, must be defined and agreed. This may involve the CSP being responsible for vulnerability assessment and patching for some or all aspects of the service, depending on the cloud service model adopted (e.g. IaaS, PaaS or SaaS or similar service definitions).

2.3 Patches and updates

Patches and updates will typically be issued by software vendors on a regular schedule as cumulative packages. These will be linked to the specific version of software that they relate to and may have dependencies stipulated with other software modules, products or operating systems.

Procedures will be put in place to obtain copies of the software updates electronically when they are issued by the vendor. The scheduling of the installation of updates will depend upon several factors including:

- The criticality of the systems being updated
- The expected time taken to install the updates (and requirements for service outages to users)
- The degree of risk associated with any vulnerabilities that are closed by the updates
- Co-ordination of the updating of related components of the infrastructure
- Dependencies between updates

An update release plan must be created and maintained to keep track of when various system will be updated, taking into account the factors listed above. The plan must be managed through the change management process. For updates that are low risk and regular, a standard change may be defined within the change management process to allow this to happen without excess administrative overhead (see Change Management Process).

2.4 Vulnerability assessment

In addition to the regular application of vendor-supplied software updates, Jadarah For Dept Collections Co. will conduct a vulnerability assessment at least twice a year. The focus of the vulnerability assessment will be guided by the most recent risk assessment.

The purpose of this assessment is to identify existing vulnerabilities in systems that could be exploited by an attacker. These could include known software vulnerabilities that have not been patched, configuration errors that need to be corrected or examples of inadequate security practice that need to be addressed.

The assessment may be carried out in-house, by an external company or a combination of both and as a minimum should cover:

- Assessment of the security of all routes into the organization's internal network from the Internet
- Externally-facing web servers
- Business critical servers on the internal network
- A selection of typical user computers

If resources permit, additional areas should be assessed such as the vulnerability of employees to phishing attacks.

It is not the organization's policy to attempt to exploit the vulnerabilities found as a matter of course. This type of penetration test may be commissioned as required using external specialist resources as part of a carefully planned exercise performed outside of normal business hours. The permission of cloud or hosting providers must be obtained prior to testing starting.

2.5 Hardening

A further action that will be taken to reduce the number and extent of vulnerabilities within Jadarah For Dept Collections Co. systems is the hardening of server and other device configurations. This involves the shutting down of services and protocols that are not needed so that the attack surface is reduced.

These hardening activities will be carried out according to vendors' guidelines and under the control of the change management process.

2.6 Awareness training

As a result of a vulnerability assessment, it may be necessary to increase efforts in security awareness training for employees and contract staff. This training should explain the nature of vulnerabilities and what can be done to reduce them.

As part of awareness training, a phishing simulation exercise will be conducted on a regular basis. This will involve the sending of emails to employees that are intended to be similar to typical phishing messages, but which simply report to a central point within Jadarah For Dept Collections Co. if the requested action is performed by the employee, for example clicking on a link or opening an attachment. These exercises will help to assess the effectiveness of the awareness training delivered in recognising and avoiding malware disguised in emails.