Chapter Title	Section #		Subject #
Information Technology / Information Systems	ITIS		411
Subject Title **Penetration Testing**	Adopted 2/28/23	Last Revised 1/2023	Reviewed NEW

POLICY

Application

This policy shall apply to The Right Door for Hope, Recovery and Wellness.

1. Intent

To identify security gaps impacting the Confidentiality, Integrity, and Availability (CIA Triad) of all systems and data used by The Right Door.

2. Purpose

A penetration testing policy framework document provides guidance for managing a penetration testing program and performing penetration testing activities with the goal of improving defensive IT security for The Right Door's infrastructure, systems, services, and applications.

3. Penetration Testing Design Scope

3.1. This document defines the roles and responsibilities of The Right Door's IT security team personnel as well as external third-party security service providers.

3.1.1. The general scope of this policy applies to all equipment owned and/or operated by The Right Door, and to employees connecting to any The Right Door-owned network domains or cloud applications managed by The Right Door.

3.1.2. Defining the general scope of this policy ensures that penetration test activities are focused on relevant components and safeguard The Right Door against violating authorized system boundaries.

3.1.3. All penetration testing activity conducted on equipment owned or controlled by The Right Door must conform to all national and regional laws that govern the physical location of the asset and the nature of the data, as well as any acceptable use policy limitations imposed by the contracts and agreements

Chapter Title	Section #		Subject #
Information Technology / Information Systems	ITIS		411
Subject Title **Penetration Testing**	Adopted 2/28/23	Last Revised 1/2023	Reviewed NEW

between The Right Door and third-party infrastructure service providers and application licenses.

3.1.4. It should also be noted that this policy document does not provide a comprehensive definition of all scenarios, terminology, and activities that may be encountered during penetration testing activities.

3.1.5. Therefore, all parties should also use their best judgment when performing penetration testing activities and communication should be used to clarify any potentially conflicting situations.

3.2. Goals

3.2.1. The primary goal of The Right Door's penetration testing program is to identify security gaps impacting the Confidentiality, Integrity, and Availability (CIA Triad) of all systems and data used by The Right Door.

3.2.2. Ultimately, the discovery of vulnerabilities shall facilitate risk remediation in line with internal corporate governance objectives.

3.2.3. This includes meeting both internal risk objectives and external IT security standards including PCI-DSS for merchant payment processing and HIPAA/HITECH.

3.3. Penetration Testing Engagement Types

The Right Door's penetration testing program will include the categories of testing engagements described in the sections below.

3.4. Network Testing

3.4.1. Network penetration testing is to identify any exposed vulnerabilities and security weaknesses in The Right Door's network infrastructure that includes but is not limited to servers, firewalls, switches, routers, printers, workstations, security appliances, peripherals, and any software applications, services, or APIs within The Right Door's network environment.

Chapter Title	Section #		Subject #
Information Technology / Information Systems	ITIS		411
Subject Title **Penetration Testing**	Adopted 2/28/23	Last Revised 1/2023	Reviewed NEW

3.4.2. Both internal and external activities shall be performed as separate engagements.

3.4.3. Additionally, network penetration testing activities may include credentialed and non-credentialed testing activities to provide increased protection against attacks that may happen from sensitive internal network positions.

3.4.4. The high-level goals of network penetration testing should include testing all potential MITRE CVE vulnerabilities and attempting to evaluate the resilience against known attacker TTP included in the MITRE ATT&CK framework.

3.5. Web Application Testing

3.5.1. Web application penetration testing is to identify any vulnerability, security flaws, or threats in web applications owned by The Right Door. Activities may use any known malicious attacks on the application including both manual and automated penetration testing activities.

3.5.2. The high-level goals of web-application penetration testing should include all vulnerabilities listed in the OWASP Top Ten web-application vulnerabilities, MITRE CWE software weaknesses, and attempt to evaluate the application's resilience against known attacker TTP included in the MITRE ATT&CK framework.

3.6. Wireless testing

3.6.1. Wireless penetration tests seek to assess The Right Door's wireless network security for all of the CIA Triad components. Targets should include any workstations, laptops, tablets, smartphones, and printers, as well as any other peripherals and IoT devices. Testing activities should also comprehensively include all wireless protocols used by The Right Door's infrastructure.

3.6.2. Wireless penetration testing should verify that wireless access points (AP) are segmented with respect to guest wireless networks and internal corporate wireless networks. This includes testing that The Right Door's wireless access points appropriately restrict access to The Right Door's corporate wireless

Chapter Title	Section #		Subject #
Information Technology / Information Systems	ITIS		411
Subject Title **Penetration Testing**	Adopted 2/28/23	Last Revised 1/2023	Reviewed NEW

networks and that no information about The Right Door's internal network can be accessed by attackers.

3.6.3. Other high-level goals of wireless penetration testing are to ensure that all data passing over the wireless channels is protected from discovery by an attacker, that wireless networks are reliable and available, and that data passing over the wireless network cannot be modified by an attacker.

3.7. Social Engineering

3.7.1. Social engineering penetration testing is to increase security assurances to The Right Door's to business operations by testing personnel resilience to social engineering attacks and providing user awareness training where weaknesses are uncovered.

3.7.2. Social engineering penetration testing should include both technical and non-technical attempts to persuade or trick The Right Door's staff into performing actions that may reveal sensitive information. This should include both directly providing the sensitive information to an attacker or performing actions that may result in giving an attacker access to sensitive information such as executing files provided by an attacker.

3.7.3. The high-level goal of social engineering penetration testing activities is to educate personnel about the potential implications of the actions they perform in their day-to-day duties, and the various contexts in which a cyber-attack may involve them.

3.8. Physical Testing

3.8.1. Physical penetration testing seeks to gain access to restricted physical locations within The Right Door's buildings, critical IT infrastructure, systems, data, or employees.

3.8.2. The primary benefit of a physical penetration test is to expose weaknesses and vulnerabilities in physical controls including but not limited to locks, elevators, barriers, surveillance cameras or systems, and access control technologies such as access card readers and biometric scanners.

Chapter Title	Section #		Subject #
Information Technology / Information Systems	ITIS		411
Subject Title **Penetration Testing**	Adopted 2/28/23	Last Revised 1/2023	Reviewed NEW

3.8.3. The high-level goal of physical penetration testing is to eliminate security weaknesses that provide unauthorized physical access to The Right Door's assets.

Deborah McPeek-McFadden, Board Chairperson	Date		