MSS-DP-DOC 11.7   
DATA PROTECTION Penetration Testing

Retirement Capital

Version 1.0 June 2020

|  |  |  |  |
| --- | --- | --- | --- |
| **Classification:** | Company Confidential | | |
| **Version:** | 1.0 | | |
| **Document title:** | MSS-DP DOC 11.7 | | |
| **Document management** | Gavin McCloskey | **Authorised by:** | Gavin McCloskey |
| **Revision interval:** | Annually/ad hoc | **Last revision:** | 14/11/2020 |

# Revision History

Contents

[Revision History 2](#_Toc7761712)

[1. Management Summary 4](#_Toc7761713)

[1.1 Data Protection Act 2018 4](#_Toc7761714)

[2. Scope 5](#_Toc7761715)

[2.1 Scope 5](#_Toc7761716)

[2.2 Overview 5](#_Toc7761717)

[2.3 When are they conducted? 5](#_Toc7761718)

[2.4 Tests employed 5](#_Toc7761719)

[2.5 Test Results 6](#_Toc7761720)

# Management Summary

This document defines when and how penetration testing will be implemented in the organisation. As the organisation is new, penetration testing will no start until relevant systems are in place on 1st June 2020 and then annually thereafter unless a security incident requires and interim test.

## 1.1 Data Protection Act 2018

The Data Protection Act 2018 is the UK’s implementation of the General Data Protection Regulation (GDPR). This Data Protection Policy forms the basis for complying with legal data protection requirements as well as the protection of the processed personal data of Retirement Capital

Data protection is essential for Retirement Capital in order to meet the legal requirements for handling person-al data. This data protection Policy is therefore made binding on all the organisation’s internal pro-cesses. This is data protection by design and is fundamental to the company’s policy and attitude to data protection.

Retirement Capital is both a data controller and a data processor as defined under the Act. The former because we hold necessary data on our staff, subcontractors, suppliers and customers. The latter because we provide cloud processing services for government and private sector customers.

Under the Act, everyone responsible for using personal data has to follow strict rules called data protection principles. They must make sure the information is:

• used fairly, lawfully and transparently

• used for specified, explicit purposes

• used in a way that is adequate, relevant and limited to only what is necessary

• accurate and, where necessary, kept up to date

• kept for no longer than is necessary

• handled in a way that ensures appropriate security, including protection against unlawful or unauthorised processing, access, loss, destruction or damage

This Data Protection Policy regulates the handling of personal data. In particular, it is intended to:

• Assign responsibilities and obligations for all relevant privacy issues,

• Raise awareness of the need for strategic, technical and organisational measures to ensure data protection requirements, and

• Define the procedure for dealing with data Breach incidents.

# Scope

## Scope

Penetration testing of all systems conducted by an external company.

## Overview

Penetration testing is a systematic process of probing for vulnerabilities in our applications and networks. It is essentially a controlled form of hacking in which the ‘attackers’ operate on our behalf to find the sorts of weaknesses that criminals exploit.

The penetration testing process involves assessing our systems for any potential weaknesses that could result from poor or improper system configuration, known and unknown hardware or software flaws, and operational weaknesses in process or technical countermeasures.

An experienced penetration tester can mimic the techniques used by criminals without causing damage. These tests will be conducted outside business hours or when networks and applications are least used, thereby minimising the impact on everyday operations.

## When are they conducted?

We will carry out a penetration test:

* In response to the impact of a serious breach on a similar organisation;
* To comply with a regulation or standard, such as the PCI DSS (Payment Card Industry Data Security Standard) or the EU GDPR (General Data Protection Regulation);
* To ensure the security of new applications or significant changes to business processes;
* To manage the risks of using a greater number and variety of outsourced services;
* To assess the risk of critical data or systems being compromised.

## Tests employed

**External:** The objective of an external network penetration testing is to identify security vulnerabilities in how an organisation connects with the Internet and other external systems. This includes servers, hosts, devices and network services. If an organisation’s interfaces are not designed correctly, criminals will be able to enter the network and perform malicious activities.

**Internal:** The objective of an internal Network penetration test is to determine what vulnerabilities exist that are accessible to both an authenticated and non-authenticated user to ensure that the network is critically assessed for both the potential exploit of a rogue internal user, and an unauthorised attack.

**Web Application:** The objective of web application penetration testing is to identify security issues resulting from insecure development practices in the design, coding and publishing of software. Applications

are a vital business function for many organisations as they are used to process payment card data, sensitive personal data and/or proprietary data.

**Wireless Network:** The objective of wireless network penetration testing is to detect access points and rogue devices in an organisation’s secured environment.

**Simulated Phishing:** The objective of phishing and social engineering penetration testing is to assess employees’ susceptibility to break security rules or give access to sensitive information.

## Test Results

The external penetration tester will provide an assessment on each element, rating risks as Critical; High; Medium or Low. The results will be discussed between the DPO and the Board and any mitigating or corrective actions agreed.