Penetration Test Scoping

Company Name:

Subject:

Date:

Author:　　　　　**Timeless IT Business Limited**

Please contact Daniel Wright at support@timelessims.co.uk if you have any questions on completing this form or fill it in and we will contact you if we need clarification once submitted.

Introduction

Overview

The following document outlines pre-engagement questions for producing a quote and scope of works for conducting a penetration test.

Contents

The questions asked in this document will cover points of contact, timeframes, types of testing required, and any information regarding or required for testing.

Penetration Testing Scoping Questionnaire

Contact Details

Main Contact Name:	
Company Name:	
Address:	
Telephone Number:	
Mobile Number:	
Email:	

Type of Service(s) Required

Website/Web Application Penetration Testing	
Wireless Penetration Testing	
Networking Device Review	
Social Engineering Phishing Emails	
External Infrastructure Penetration Testing	
Internal Infrastructure Penetration Testing	

Commercial in Confidence
Chapel House, 21a Woodthorpe Road, Ashford, Surrey TW15 2RP Tel: 0800 328 2852 www.timelessims.co.uk
Your outsourced IT Director

Timeless IT Business Limited Registered in England at Gladstone House 77-79 High Street, Egham, England, TW20 9HY.
Under Company number 07236106. ' Timeless ' and 'Timeless IMS' are trading names of Timeless IT Business Limited.

Code Review	
Staff Security Awareness Training	

Timelines

ASAP	
In the next month	
In the next 3 months	
In the next 6 months	
Outside of working hours required (please specify below)	

Website/Web Application Penetration Testing

Target URL(s)	
Target Sub Domain(s)	
Low Level Credentials (if required)	
Number of static pages	
Number of dynamic pages	
Are there any areas that are specifically out of scope? (please specify)	
IP Address of the hosting server	
Nature of the environment being tested (Production/Staging/Development/Live)	
Any other details not previously mentioned (please specify)	

Please Note: If the site hosted by a 3rd party IT/Web hosting provider, we will require evidence that they have been notified and have given permission for the testing to be performed. Throughout the test we may utilise login credentials for application and website testing, a secure method of exchanging these details will be arranged between Timeless IT Business Limited and the client.

If any network protection methods (i.e. IPS, WAF, IDS) are used, IP addresses associated with testing may require IP whitelisting. If so, this information will be provided prior to the test commencing.

Wireless Penetration Testing

Names of Wireless SSID(s)	
Number of locations POPs	

Networking Device Review

Please list the devices in scope (type & vendor)	Device Type	Manufacturer	Quantity
If enforcing access controls/filtering, what type of filtering and approx. how many rules are configured within each device's policies?			
Will they be reviewed onsite or offsite? (If offsite, please state a preferred connection method)			

Social Engineering Phishing Emails

Email address(es) of the targeted employees. (Chosen employees should be selected from a varied range of departments and levels of authority)	

External infrastructure Penetration Testing

External Facing IP Address Ranges	
Please list which of the above IP addresses are live	
Are there any IP Addresses that are specifically out of scope? (please specify)	

Internal Infrastructure Penetration Testing

Number of Servers (please include Virtual Hosts)	
Internal IP address(s) of server(s)	
Number of Physical Sites	
Types of inter-site connectivity currently in use (if applicable)	
Number of End-point Devices	
Are End-point devices built from a standard client image?	
Internal IP address range of end-point devices	
Are there any IP Addresses that are specifically out of scope? (please specify)	

Code Review

Number of lines of code (approx.)	
Languages(s) used	
3rd party / Open Source Components	
Test Environment Provided (Yes/No)	
Design documents provided (Yes/No)	

Staff Security Awareness Training Course

Number of Employees to attend	
Training to be held on-site or off-site	
Preferred date	

Additional Questions

Upon penetration of a device/service/personnel would you like testing of that vector to be stopped and reported there or for further penetration testing to be done via that vector? (e.g. Privilege Escalation)	
Internet facing service list (e.g. email server, file server, VPN, intranet, services in DMZ, timesheet app, ERP, staging server, ticket/task tracking system)	
Any services running in the cloud? (e.g. Microsoft Azure, Amazon Web Services)	

Additional Information