Williams & Wilson

IT POLICY AND BUSINESS CONTINGENCY & DISASTER RECOVERY PLAN

Williams & Wilson Limited
(the "Company")

Table of Contents

IT Policy

Williams & Wilson Limited (the "Company") shall have adequate means for the protection of client records and information and shall perform monthly security patches.

1. Server
The Company shall have in place a safe and secure server being located at 292/10 Republic Street, Valletta, Malta, VLT 1011 and managed by Smart Studios.

2. Secure Perimeter
The Company shall apply a secure perimeter policy to the internal network. The Company's internal network shall be hidden behind secure firewalls, with access control to authorized officers only.

3. Server Room Access
Access is limited to qualified and trusted personnel only.

4. Internal Domain
Personnel can only access PCs using their work credentials. Active Directory to authenticate users. USB usage is highly restricted.

5. Firewall Protection
There will be Firewall Protection on network and users.

6. Secure Data Storage
Data shall be securely backed up on a daily basis on server and on cloud for redundancy and to support a Disaster Recovery scenario. There will be daily automatic data back – ups.

7. Risks against Malware, Phishing, Man in Between, Ransomware, Spyware
AVS software and Firmware up to ISO27001 standard. DDoS Protection for Infrastructure and Web Application attacks using Cloudflare; Audit and Compliance tools related to vulnerability scanning using F-Secure Radar and Acunetix; Centralised Event Log Management Services using GrayLog; Web Servers based NGINX, Apache, IIS, and Web Application Firewalling shall be installed to ensure uniformity in network protection. The Software shall be used as Antivirus, antimalware and anti-spyware.

Staffs shall be made duly aware of the above risks and constantly reminded about these risks.

To ensure the smooth running of this IT Policy, all users shall be provided with the requisite training.

8. Audits
The Board of Directors shall request their IT professional to conduct the following on a regular basis:

(a) regular IT audits and to address identified loopholes accordingly; and
(b) conducting penetration testing to ensure that their systems are not vulnerable or susceptible to cyber-attacks.

9. Business Contingency & Disaster Recovery Plan

The purpose of this Business Contingency Plan is to define the recovery process developed to restore the Company's critical business functions in the case of natural disasters or other matters that cause disruption to the Company's business such as fire, etc. This plan details the Company's procedures for responding to an emergency situation which affects the Company's ability to deliver core services to its customers or its ability to operate.

Objectives of the Plan

a) Facilitate timely recovery of core business functions and data
b) Protect all information related to customers, clients and employees
c) Minimize loss of data
d) Minimize the critical decisions to be made in a time of crisis

The Company will have all information, documents, data etc CRM Software hosted in Webserver location in Malta which shall be accessible anytime irrespective of any disaster.

10. Technical specification

There is the option of plug in and continue operations from any location with internet access. In house web based CRM Software built and provided by [To be determined at a later stage] with all security feature and managed 24x7 for storage of all client information and documents safety with all security software installed.

11. Security, Back up plans and Disaster Recovery

The CRM Software hosted and maintained cloud security system refers to the broad set of policies, technologies and controls that the company will use to protect its data. Systems that the Company uses are SSL, Permission based admin, encrypted passwords and Cloud based server.

The Company has an automatic backup system in its control panel which backup the database daily thereby enabling the creation of a duplicate instance or copy of a database in case the primary database crashes, is corrupted or is lost.

12. Business Contingency Planning Team

The following individuals are designated plan coordinators and are responsible for the execution of this plan in the event of disaster.

Name	Title	Email
Mr. Robert Ryan Porter		ryan@theporterfamily.me.uk

In the event of an emergency, staffs of the Company will be required to contact anyone from the Business Contingency Planning Team.

13. Staff Awareness

The Manager will always ensure that all staffs are made aware of this Business Contingency and Disaster Recovery Plan and their respective roles and obligations.

Williams & Wilson

Premier Business Centre, 10th Floor Sterling Tower, 14
Poudriere Street, Port Louis, Mauritius
Tel: +44 203 996 1492
E-mail:admin@williamsandwilson.org
Website: www.williamsandwilson.org