



**TITAN PERFORMANCE**

Titan Performance Gyms Ltd

**DATA SECURITY POLICY**

# Titan Performance Gyms Ltd

## DATA SECURITY POLICY

Titan Performance Gyms Ltd is committed to respecting and securing the privacy of all our members, coaches, self employed trainers using the site and it's visitors. At times Titan Performance holds a large amount of valuable user data which could be a target for any cyber attacker looking for data to sell, make fraudulent purchases or to breach other accounts.

### 1. Statement of Intent

Titan Performance Gyms Ltd will:

- ensure all that require it receive appropriate training in the protection of sensitive data;
- review handling procedures for sensitive information and place security as a standing item on Management meeting agenda to ensure these procedures are incorporated into day to day practice.
- Hold this security policy document somewhere accessible for all to read.

### 2. System Password security

All users of our internet and management systems are responsible for taking the appropriate steps, to select and secure their passwords.

### 3. Anti-virus policy

- All machines must be configured to run the latest anti-virus software. The antivirus should have periodic scanning enabled for all the systems.
- The antivirus software in use should be cable of detecting all known types of malicious software (viruses, Trojans, adware, spyware, worms and rootkits)
- All removable media (for example USB drives and others) should be scanned for viruses before being used.
- All the logs generated from the antivirus solutions have to be retained at a minimum requirement of 3 months online (for PCIDSS requirements) and 1 year offline.
- End users must not be able to modify and any settings or alter the antivirus software.
- E-mail with attachments coming from suspicious or unknown sources should not be opened. All such e-mails and their attachments should be deleted from the mail system as well as from the trash bin. Never forward any e-mail if you suspect it contains viruses.

#### **4. Roles and Responsibilities**

The Digital Officer (Ben Caton) is responsible for overseeing all aspects of information security, including but not limited to:

- Creating and distributing security policies and procedures.
- Monitoring and analysing security alerts and distributing information to appropriate information security and business unit management personnel.
- Creating and distributing security incident response and escalation procedures that include:
  - Maintaining a formal security awareness programmes for all and also providing multiple methods of communicating awareness (for example, posters, letters, meetings).  
Ensuring that all acknowledge in writing at least once that they have read and understand the Company's data security policy.
- Titan Performance Gyms Ltd shall maintain daily administrative and technical operational security procedures that are consistent with the PCI-DSS (for example, user account maintenance procedures, and log review procedures).