IT Security Policy

This document is prepared and managed by 4 global and is intended for users and system administrators and relates to the IT security standards maintained across all platforms developed by 4 global.

The current version is available from the 4 global web pages.

Change History:

	Date	**Status**	**Responsible**
Original	May 2015	Issued	Utku Toprakseven
Revised	May 2016	Issued	Utku Toprakseven
Revised	May 2017	Issued	Utku Toprakseven
Next revision	May 2018		

4 global's Views on Information Security

4 global is committed to ensuring the integrity of the information generated and stored within their online platforms and compliance with relevant legislation covering this area. To maintain this integrity in what can be regarded a transient medium 4 global believes that it is essential to establish and conform to clearly defined standards of operation in relation to platform-based information. To assist with this 4 global has developed this IT Security Policy, which will be reviewed and updated annually.

4 global also aims to make its Employees and Users of their platforms aware of this Policy and also of other relevant standard practice and legislation, and how to achieve compliance with them.

Policy Statement on Information Security

(1) 4 global seeks to ensure that all information generated and stored within their online platforms developed by the company is accurate and appropriately available.

(2) All clients, partners and employees with access to the information kept within 4 global platforms will conform to the IT Security Policy.

(3) All data connections to external bodies will be validated to conform to the IT Security Policy.

Principles of Implementation

Scope

The IT Security Policy covers all online platforms developed by 4 global. All new systems must have their security controls agreed by the Director of Sport Intelligence, or nominee.

The Policy is available on the 4 global's website for anyone wishing to view them.

The IT Security Policy may be changed at any time in order to maintain currency as technology changes or as new threats emerge. Users will be informed appropriately.

Conditions

- All systems within the company and connections to outside bodies must conform to this Policy. 4 global will ensure that the Policy is put into practice.
- 4 global reserves the right to isolate any system or network that represents a potential or actual breach of security.
- 4 global reserves the right to monitor information sent over its networks.

Access Control

- All platforms, except those designed for public open access, are required, at their point of entry, to have an auditable sign-on procedure with a unique, traceable Identifier and Password.
- All access to platforms will be audited to ensure traceability and responsibility.

- Access and connection to selected wider networks will be restricted to authorised Users only.
- 4 global reserves the right to deny systems access to users.

Security Breach Handling

4 global, or a party designated by it, will be responsible for and/or deal with:

- All incidents that affect, or could affect, information security.
- The monitoring of security breaches.
- Maintaining the *IT Security Policy* document.

Data Protection

Users who input data on to 4 global's online platforms are responsible for ensuring that they comply with the requirements of the Data Protection Act.

Other legislation to consider:

- Computer Misuse Act 1990
- Malicious Communications Act 1988
- Regulation of Investigatory Powers Act 2000
- Freedom of Information Act 2000
- Privacy and Electronic Communications (EC Directive) Regulations 2003
- Terrorism Act 2006 s3
- Police and Justice Act s35-38

Responsibility

- Responsibility for compliance with the policy is delegated to Sport Intelligence (SI) team members within their respective roles.
- Individuals are responsible for their own actions and usage of their assigned Personal Identifier.
- Individuals are responsible for ensuring that they comply with all the requirements of the IT Security Policy.

All User queries and notifications relating to the contents of this document should be addressed to 4 global Customer Support by email to support@4global.com

Table of Contents

4 global uses London based cloud servers provided by DigitalOcean (the “Provider”). All of Provider’s datacenters in the London, New York, San Francisco, Singapore, London and Amsterdam have been certified by national and/or international security standards. The London facility is ISO9001:2008, ISO27001, and SSAE16 / ISAE 3402 certified.

The security guidelines 1-5 below are taken from the Security Policy of the Provider and can also be found at https://www.digitalocean.com/security.

1. Virtual Server Security & Employee Access

Virtual server security and data integrity is of the utmost concern for the Provider. As a result none of the Provider’s technical support staff have any access to the backend hypervisors where virtual servers reside nor direct access to the NAS/SAN storage systems where snapshots and backup images reside. Only the Provider’s engineering team has direct access to the backend servers.

2. Physical Security

The Provider uses only premier datacenter facilities for colocating our equipment including: Equinix, Telx, and Telecity. Each site is staffed 24/7/365 with onsite security and to protect against unauthorized entry. Each site has security cameras that monitor both the facility premises as well as each area of the datacenter internally. There are biometric readers for access as well as at least two factor authentication to gain access to the building. Each facility is unmarked so as not to draw any additional attention from the outside and adheres to strict local and federal government standards.

3. Credit Card Security

The Provider hands off credit card processing to Stripe. They power online transactions for thousands of business and SaaS platforms and comply with PCI standards in the storage and handling of credit card information. For PayPal transactions the Provider pass off customers directly to PayPal who is also PCI compliant.

4. Communications

All communications with DigitalOcean are transmitted over SSL (HTTPS) for both access to the public website as well as the API. The Providers provides connectivity to the virtual servers via SSH and recommends that customers use SSH keys to setup their access.

5. Snapshot and Backup Security

Snapshots and Backups (images) are stored on an internal non-publicly visible network on NAS/SAN servers. Customers can manage directly in how many regions their snapshots exist which allows customers to increase the redundancy of the files that are stored in the backend.

6. Access Controls

General

4 global platforms will have appropriate access controls. These controls will be defined for access to the entire platform, database, specific data files, software applications, email and other resources. Access controls can be specific to individual Users or to groups of Users. Users will only be permitted access to those files and system resources they need to perform their job functions.

In a platform environment, considerations will include:

- Identification of the User to the platform by Username and Password
- Access to *required* Files and Folders
- Account Restrictions
- Time Restrictions (set times of day between which the account may be used)
- Access to Databases and associated Applications Software
- Other Privileges

Access controls on User Accounts

6.1 Individual Users will each be given a personal account for which they are held responsible.

6.2 Group accounts will be permitted where necessary for specific purposes, but they will be suitably limited in function. By definition, a group account is used by more than one authorised person, which makes it harder to determine who performed any specific action. Users of any group account must understand their responsibilities for its security and only use it in the manner agreed.

6.3 A group account may be withdrawn if, in the judgment of 4 global, the account or the manner in which it is used is thought to present a security risk.

6.4 User accounts will be reviewed on a regular basis, and any accounts that are no longer required will be removed. See the section, “User Identification and Authentication” for further details.

6.5 A User account will not be allowed more than one login session at a time except where absolutely necessary for specific work to be performed.

System Administration

6.6 Sensitive system commands and software will be restricted to system administrators and security personnel.

6.7 Accounts with enhanced file access rights or with high level access to platforms will be used only when necessary to perform tasks requiring such access.

Permitted Use

6.8 All users of 4 global platforms must adhere to the rules set out in this IT Security Policy.

7. User Identification and Authentication

User identification and authentication is the ability to identify the User to the online platform and to confirm the claimed identity of the Users. The User identifies him/herself to the platform by entering a Username, usually consisting of his/her email address. The User's identity is authenticated when the User enters a valid password.

User Registration

7.1 The Platform Administrator creates User accounts and emails his/her Username and Password to each User.

User IDs

7.2 Each User will have one and only one Username and it will be unique within the computer system.

7.3 All Usernames will have expiry dates. These will be enforced by technical means where possible.

7.4 Expired Usernames will have their access to computer systems suspended and deleted dependant on criteria according to User type.

7.5 User types fall in to one of three categories; admin, user and demo.

7.6 Admin accounts are only accessible by 4 global and its official partners and used to manage accounts within the online platform.

7.7 User accounts are expired at the end of subscription date and then deleted 3 months after the account expires.

7.8 User accounts are deleted when the account has not been logged into for 12 months.

7.9 Accounts known as "demo" accounts are merely external accounts with short lifetimes and specific access rights granted to allow the authorised users, typically prospect clients to test the user interface and functionalities.

User Passwords

7.10 User passwords must be known only to the User and stored in an encrypted way within the platform database.

7.11 The User's supervisor or the platform administrator does not need to know a User's password and will not ask for it.

7.12 The User has no need to and must not divulge their password to another party.

7.13 Passwords will not be echoed to the User's screen when they are keyed in.

7.14 When a User forgets his/her password, the administrator will issue a temporary link and send it to the User's email address, which is also his/her username within the platform.

7.15 The User will be able to change his/her own password without administrator intervention.

7.16 The User will be required to follow good security practices in the selection and use of passwords.

7.17 User will be required to use passwords, which are at least six characters long.

7.18 Passwords should include both alphabetic and numeric characters.

- The User is warned against using “weak” passwords that may be obvious and guessable words.
- Other examples of weak passwords include the following:
  - Month of the year, days of the week or any other aspect of the date.
  - Family names, initials or car registration numbers.
  - Telephone numbers or similar all numeric groups.
  - More than two consecutive identical characters

7.19 If suspicion arises that a password may be known to an unauthorised party, the password should always be changed immediately and without regard to whether a regular periodic password change is due.

Periodic Changes of Password

7.20 Where technically possible, the platform will require periodic changes of the User’s password. Sixty days is the recommended password change interval. Where it is not technically possible to enforce periodic password changes, regular changes should be encouraged by User education.

7.21 The User will be required by the platform administrator to choose a password different to the one previously used.

7.22 Where technically possible, the User will not be able to use expired passwords as the new password when the system forces a password change.

8. System Administration

Assigning administrative responsibilities for the computer system is absolutely necessary in order to maintain platform security.

The System Administrator

8.1 The responsibility for the administration of the computer system, including security administration, will be assigned to knowledgeable individuals and authorised by the the Director of Sport Intelligence.

8.2 The administrator will be aware of his/her responsibilities regarding administration of the computer system as well as the security and integrity of the data and information stored and processed on the computer system.

8.3 System administrators will be provided with the proper training, including training on security issues where required.

8.4 System administration will take place on secure workstations using secure IDs assigned to individual administrators as per the system administration rules.

8.5 System administrators will be aware that operational shortcuts can lead to errors and reduce effectiveness of safeguards or even negate them.

9. Responsibility for Review

The Director of Sport Intelligence is responsible for the maintenance and [annual] review of this Policy.