



HealthcareBookings.com – Security Set Up

Introduction	2
Overview of the process for using HealthcareBookings.com	2
Professionals	2
Patients	3
Passwords	4
Hosting Security	4
Overview of Digiweb hosting facility	4
Connectivity	5
Power.....	5
Network Operations Centre	6
Fire Protection Systems	6
Cooling Systems	6
Backups	7
Security Updates.....	7
SSL Cert.....	7



Introduction

IMTS acknowledges the need for extremely tight security surrounding the HealthcareBookings.com website. Given the nature of the data being stored and processed it is vital that it is handled in the most secure manner possible.

The purpose of this document is to outline the various security measures that will be taken into account for this system.

Overview of the process for using HealthcareBookings.com

Professionals

Professionals (Consultants, GPs and Hospital Administrators) can register to make their services available to the general public via the website. They do this by filling in a registration form on the website:

Register

Please enter your registration details in the form below and click **Register**.
Fields marked with an * are mandatory.
If you are not a Healthcare Professional please [Register Here](#)

Registration Details

First Name *

Surname *

Address *

Work Telephone *

Mobile

Email *

Profession *

Secretary

Biography *

? A simple overview will suffice

Add photograph

[Cancel](#)



Once they have registered their details are forwarded to the site administrator who vets their credentials before activating their account on the website. Once activated, they can log into the Professional Dashboard to input availability for their services using a series of calendar and form-driven controls. Their services are then made available to the general public on the website via a set of search engines.

Patients

Patients can also register on the website to avail of the services provided by the professionals by filling in a simple registration form:

Register

Please enter your registration details in the form below and click **Register**.
Fields marked with an * are mandatory.
If you are a Healthcare Professional please [Register Here](#)

Registration Details

First Name *

Surname *

Date of Birth *

General Practitioner

Phone number

Mobile number *

Email *

[Cancel](#)

Once they have registered they can make bookings for the professional services that have been made available on the website.



Passwords

Passwords will be created and managed as follows:

1. Each newly registered user will be issued an individual login via an automated email in the case of Patients or an email manually initiated by the System Admin in the case of Consultants, GPs and Hospital Administrators.
2. Users will be given the opportunity to change their password at any given time once they are logged into the website.
3. Strong passwords must be used, at least 7 characters long. They must also contain a number and one of the following special characters: @#!\$%&'*^

Hosting Security

Overview of Digiweb hosting facility

The data centre building is fully owned and operated by Digiweb. As such they have been able to introduce a very high level of security.

They are located in the College Business & Technology Park in Blanchardstown. The park is a gated community with uniformed security at the front gate. Throughout the park are high definition CCTV cameras and security guards make regular patrols of the park. Access to the Digiweb building is controlled by security guards. Beyond that, access to the data centre is allowed only to authorised Digiweb staff, their guests and authorised customers. This is enforced via a swipe card system. All entrances and exits to the building are monitored by CCTV. Access to the data centre is behind a number of security controlled doors. Visitors must be on a pre-approved list of authorised visitors specified in advance.

Upon arriving at the data centre visitors are required to produce photo ID and provide the pre-arranged pass phrase for their visit. Each row of the data centre is equipped with CCTV. All CCTV cameras are monitored from the NOC and from the security at the front desk.



Connectivity

Digiweb guarantee 99.99% uptime for network and power. To ensure they exceed that guarantee Digiweb has redundant protected fibre paths feeding the data centre from their own 148 kilometres Dublin metropolitan fibre ring and from ESB telecoms fibre over a completely diverse route.

Digiweb is also peering with INEX and Packet Exchange eXpress. You can find a list of their INEX peering partners, such as Cable & Wireless, Data Electronics, HEAnet, Microsoft and Verizon Business here:

<https://www.inex.ie/about/memberlist>

Digiweb also has a microwave link located on the roof of their building, operating in the Gigahertz spectrum. Digiweb employs a dedicated IP networking team of 11 qualified staff, lead by a Cisco Certified Internet Engineer (CCIE). Network monitoring and remote hands and eyes support is provided by their Network Operations Centre (NOC). The NOC is staffed 24 x 7 x 365.

Power

Digiweb guarantees power for all customers. This is provided by an on-site dedicated ESB substation, a backup 10,000 litre diesel tank and generator, multiple Uninterruptible Power Supply (UPS) units with transformers as well as 10 tonnes of batteries.

In the event of an ESB utility power outage their supply is maintained by their back up systems. If there is an ESB utility power outage their batteries immediately take the load of all critical equipment. At the same time their generator will automatically commence operation. The generator will re-charge the batteries as well as be able to supply full power to the data centre for over 72 hours.

In the unlikely event that the utility power is going to be out for longer than 72 hours, a 24 x 7 x 365 fuel oil delivery contract (with SLA) is in place with a local reputable supplier. This supplier has three depots no more that 30 miles from the data centre and can refill the tank in less than 4 hours. It is also a policy of Digiweb that when the tank is at 60% that it is refilled.

Digiweb has scheduled regular maintenance and testing on all power related equipment. High priority contracts are in place with contractors to allow for 24 / 7 call out if required.



Network Operations Centre

Digiweb's NOC is staffed 24 / 7 by skilled server and network technicians, who proactively monitor and support their hosting customers. NOC staff also monitor the data centre network, infrastructure and environment as well as monitor the entire country-wide broadband network including the Digiweb owned 148 km fibre ring around Dublin.

Fire Protection Systems

Digiweb employ both an active VESDA fire detection system and a passive fire alarm detection system. VESDA is an active aspirating smoke detector system, in such that it draws in air from various points in the data centre and utilises a solid state laser, tuned to detect the extremely small particles of combustion. Digiweb also have a passive fire alarm system installed in the data centre and surrounding areas.

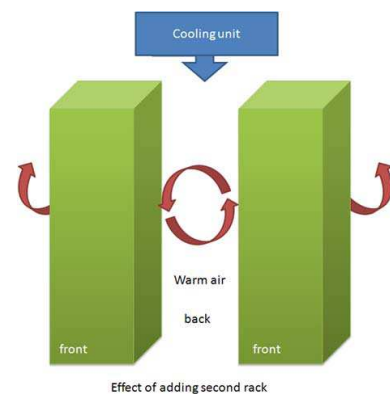
How Vesda Works:

1. Continually drawing air into a pipe network attached to a detector unit.
2. Passing the air through a dual stage filter to remove dirt
3. Sending the clean air to a laser detection chamber for smoke detection.
4. Measuring the light scatter caused by any smoke
5. Processing the detector signal and presenting the smoke level graphically
6. Communicating the information to a fire alarm control panel, a software management system or a building management system.

Cooling Systems

Digiweb utilises twelve lots of high power DX chiller units. This offers N + 2 redundancy. The chiller units are 40 KWatt each and use individual refrigeration circuits and no one unit is dependant upon the other. Each unit is fed from different breakers.

Digiweb has arranged the data centre in a hot row / cold row configuration to maximise airflow. Their cabinets were custom made for Digiweb and were built with air grilles for directing chilled air. This has resulted in 75% more air flow. Environmental factors such as temperatures are monitored 24 / 7 by their on site NOC staff.





Backups

A SQL Backup is run every night at midnight and stored onsite and offsite for disaster recovery and rollback when necessary. The same goes for files stored on the webserver, both of which are stored on site and offsite, backed up daily.

In terms of how the data gets from the production environment to the offsite backup, it is first encrypted by 128-bit symmetric key encryption (AES, TripleDES, TwoFish) and then sent as a direct file transfer down a data line to a Data Electronics facility in Kilcarbery Park, Dublin 22. The traffic itself is encrypted by 1024 bit RSA public key encryption.

In terms of security at the stored location itself, Data Electronics have not encountered a security breach since opening the Kilcarbery Park centre in 2001 and this is accredited to the high level of training conducted between their 3rd party security partners and their staff. The security policy is constantly reviewed to ensure the service remains flawless.

The Kilcarbery Park Data Centre is located within a secure business campus in west Dublin - fully monitored and managed on a 24x7 basis by a leading security company. This well established company also provide manned security personnel within the data centre itself.

In addition, Data Electronics have over 100 motion sensitive CCTV cameras, operating on a 24x7 basis, mounted both internally and externally around the data centre. All footage is recorded and stored for a 30-day period at their Network Operations Centre (NOC). All footage is available for viewing by their clients.

Security Updates

Critical security patches are deployed immediately while less critical ones are applied weekly. All updates are deployed and tested on our staging server before being deployed on the production server. Anti-virus updates are handled at Firewall access and are deployed in real-time.

SSL Cert

IMTS will be using an SSL Certificate in order to ensure the safety and security of customer details. It uses 128-bit SSL ("Secure Sockets Layer") encryption. This means that our server and site users' browsers create and agree on an encryption key that will be used only for that particular session. Once established, this key encrypts all communication between our server and the site user's browser.