PROPELLER

2018 Company Policy Documents

30th September 2018

Applications and Hosting Policy

PROPELLER

Applications and Hosting Policy Document

A requirement of the Company is to provide a secure hosting environment for it's clients. The Company regularly undertakes formal risk management reviews and these have identified that the speed, security and reliability of the service is a fundamental requirement of its own success.

Consequently, the board of directors have developed robust procedures and have forged strategic alliances with a number of reliable and highly competent organisations to ensure that it maintains a best practice approach in this area. The basis of the service is to ensure that it's customers enjoy uninterrupted access to the applications that it provides or web sites that it host's. The Company overall strategic objectives for the system are identified below:-

- That they be available for use from any location with an internet connection twenty four hours a day, seven days a week with the exception of pre-communicated outage periods for the purpose of planned maintenance and upgrades;
- Be designed and maintained in such a way that no single point of failure exists within the overall system architecture;
- Be regularly tested during simulations and fire drills that form a part of it's overall business continuity plan;
- Have sufficient processing power and be designed in such a way to ensure that they work quickly and efficiently;
- Have sufficient hard storage space to cater for the requirements of its own and its customers needs;
- Be secure against third party attacks;
- Be backed up through the use of a mirrored array meaning that single component failure neither interrupts the service nor losses data;
- Be daily backed up to a further hosting facility as a further insurance against component or hardware failure;

Taking into account the importance of the issue, the Managing Director undertakes detailed review of the arrangements on a quarterly basis, as well as unannounced audits of the strategic partners' arrangements bi annually.

The full roles and responsibilities of the partners is documented and attached to this policy. The policy is reviewed, amended and signed off annually or when considered appropriate by the board of directors.

A D Hammond
Managing Director

Hosting Arrangements

The latent risks to our hosting systems can be categorised into defined areas. For our applications to be delivered effectively we ensure that:-

- We always have sufficient power available to run our computer array;
- The array is located in a controlled, secure environment free of dust and at a pre-determined temperature;
- That we have multiple options for connection to the internet at sufficient speed and band width to meet our clients requirements;
- That regular penetration testing is conducted of the network and the applications themselves;

The Company maintains ongoing relationships with three strategic partners in order to deliver the service, with each partner responsible for a defined area of expertise.

Data Centre

Telecity Group - TelecityGroup is Europe's leading provider of premium carrier-neutral data centres, operating facilities in city locations across Europe.

TelecityGroup's data centres provide secure and highly-connected environments for the IT and telecoms equipment that powers the digital economy. The data centres are enabling environments in which the separate networks that make up the internet meet and where bandwidth intensive applications, content and information are hosted.

Our network is distributed over two top of their class datacentres in London's Docklands at Telehouse and at Telecity. Each facility is connected to each other by redundant Gigabit Ethernet circuits and each hosts autonomous services and independent external Internet connections for both international peering and global transit reach.

The datacentre themselves have stringent arrangements in place to ensure that power is always available to our computers. They maintain six independent generators capable of maintaining an uninterrupted power supply to our systems, even in the event of total power loss from the national grid. Identical arrangements are in place for environmental controls of the hosting environment.

These systems are tested on a three monthly basis with regular and planned maintenance activities undertaken to the service schedule provided by the manufacturer. A copy of their ISO registrations that cover the locations of our equipment are shown on the next page.

Lloyd's Register LRQA

Certificate of Approval

This is to certify that the Management System of:

Digital London Limited

Trading As: Digital Realty

40 Gracechurch Street, London, EC3V 0BT, United Kingdom

has been approved by LRQA to the following standards:

ISO 14001:2004 | ISO 22301:2012 | ISO 50001:2011 | ISO 9001:2008 | ISO/IEC 27001:2013 | OHSAS 18001:2007

David Derrick
Issued By: Lloyd's Register Quality Assurance Ltd

This certificate is valid only in association with the certificate schedule bearing the same number on which the locations applicable to this approval are listed.

Current Issue Date: 21 October 2016
Expiry Date: 20 October 2019
Certificate Identity Number: 10006279

Original Approvals:
ISO 14001 29 June 2010
ISO 22301 31 October 2012
ISO 50001 21 October 2013
ISO 9001 13 January 2010
ISO/IEC 27001 22 March 2006
OHSAS 18001 29 June 2010

Approval Numbers: ISO 14001 – 0015787 / ISO 22301 – 0015783 / ISO 50001 – 0015785 / ISO 9001 – 0015786 / ISO/IEC 27001 – 0015784 / OHSAS 18001 – 0015788

UKAS MANAGEMENT SYSTEMS
001

Lloyd's Register Group Limited, its affiliates and subsidiaries, including Lloyd's Register Quality Assurance Limited (LRQA), and their respective officers, employees or agents are, individually and collectively, referred to in this clause as 'Lloyd's Register'. Lloyd's Register assumes no responsibility and shall not be liable to any person for any loss, damage or expense caused by reliance on the information or advice in this document or howsoever provided, unless that person has signed a contract with the relevant Lloyd's Register entity for the provision of this information or advice and in that case any responsibility or liability is exclusively on the terms and conditions set out in that contract.
Issued By: Lloyd's Register Quality Assurance Ltd, 1 Trinity Park, Bickenhill Lane, Birmingham B37 7ES, United Kingdom

Page 1 of 10

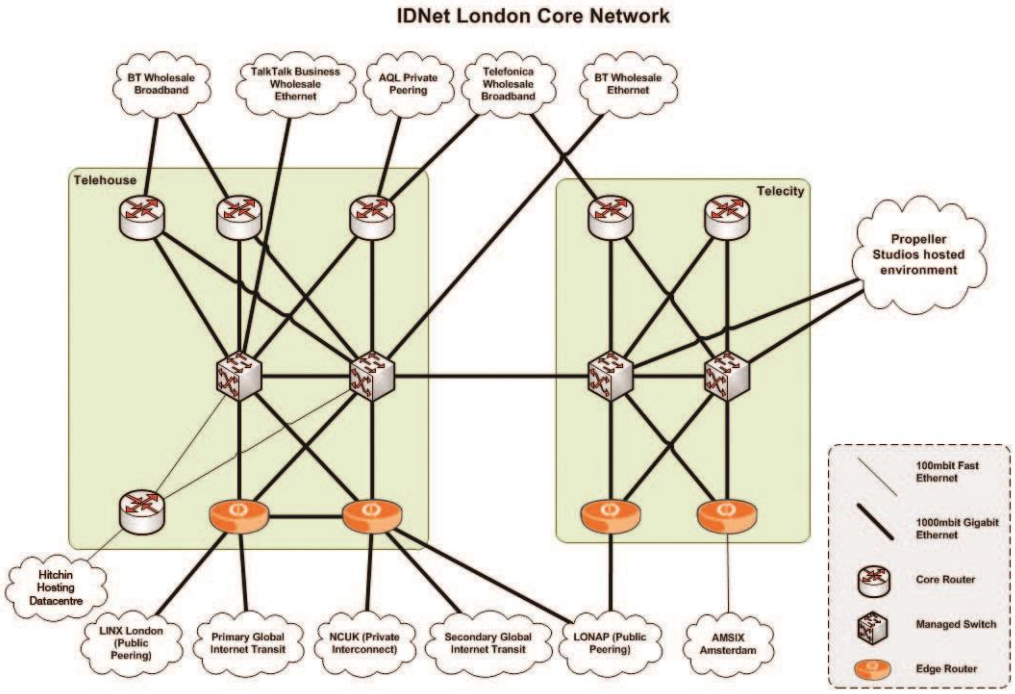
Internet connectivity

IDNet - Established in 1996, IDNet is a leading technology-driven Internet Services & Communications Provider (ISP/CP), delivering high performance data & telecoms solutions for a multitude of businesses, blue-chip corporations and government agencies throughout the UK.

Their core global Internet connectivity is presented in London at LINX & LONAP, and in Amsterdam at AMS-IX, where they have multiple transit and peering connections with over 500 global networks, enabling them to deliver data from around the world at incredibly fast speeds.

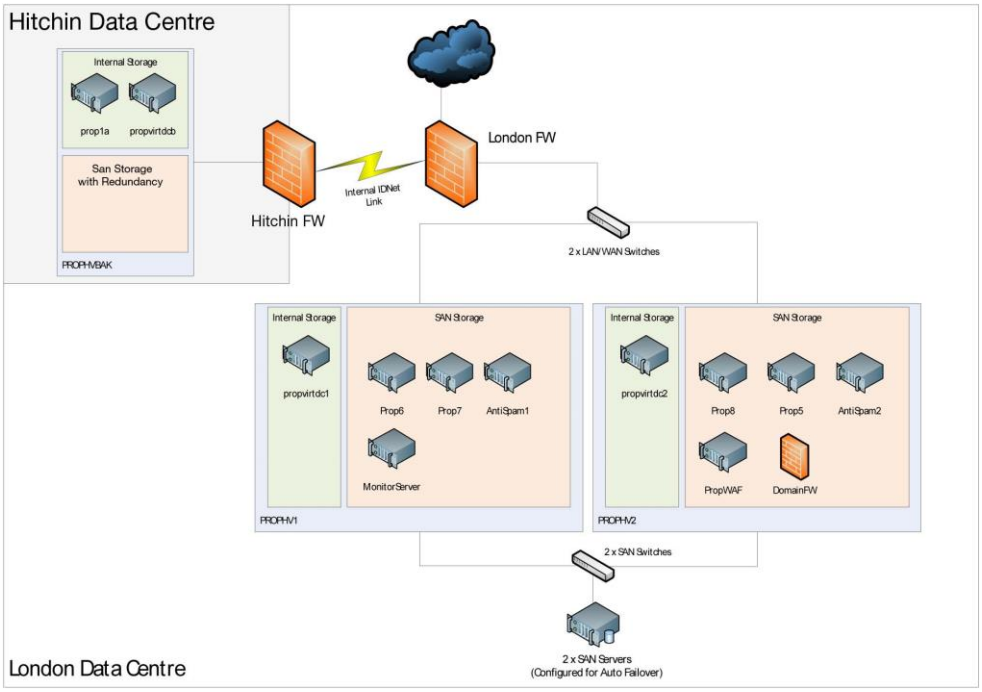
All external circuits are duplicated to ensure redundant failover in the event of an outage. In order to ensure that their own internal network can survive unexpected equipment failure every router and switch is deployed as a pair working in tandem. Should a device fail then their core network will automatically self-heal to route traffic around the problem, maintaining full service, allowing them to replace and repair the fault without disrupting normal operations.

The core network and external connectivity is monitored 24/7 with alerts issued to duty engineers in the event of a failure or unusual traffic event. Where a circuit regularly reaches 70% utilisation the capacity of that link is increased to provide sufficient headroom again.



Our own Server Array

The Company has continually reviewed and improved its own arrangements for the maintenance, security and backup of the network of computers that make up its hosting array. The schematic diagram below depicts the way in which the system is configured.



The primary array – This network of computers, switches, firewalls and hard storage units make up the day to day system that delivers the companies application hosting services.

The secondary array – This network of computers is located at the companies own datacentre in Wilbury Way, Hitchin and acts as our third level backup and Escrow solution in the event of Propeller Studios Ltd entering into administration.

The Primary and Secondary Array

The Primary hosted virtualisation platform has been designed to deliver the following:

- Fully Redundant infrastructure
- A high level of security
- Flexible server infrastructure, allowing hot upgrades with minimal downtime
- Flexible, upgradable and resilient storage
- Redundant backups both onsite and offsite
- 24 hour on call support service

The Primary array has been designed so that no single piece of hardware can cause a system wide failure of any service. Utilising the Microsoft Hyper-V 2012 R2 platform and Open-E VSS V6 SAN storage devices, automatic failover of key hardware has been designed, and tested, so that the virtual servers will automatically switch to the live server in the event of a hardware failure.

The hardware is connected using multiple switches configured in a crossover setup. This adds the ability for any single network device to fail without interruption to service. The largest impact that will be felt will be a slight data access performance degradation if a SAN switch is compromised.

All data at the Primary array is backed up locally, and then transferred to the Secondary array (Hitchin Disaster Recovery site) during off peak times where historic copies of data are stored.

In the event of any failure our engineers are contacted by email and text message with the details of the failure. They will then respond to any support call within their SLA times:

- 8 – 6 Monday to Friday:
    - Critical Failure : 30 minute response
    - Other Failure : 1 hour response

- 24 Hours:
    - Critical Failure : 1 hour response
    - Other Failure : 2 hour response

In most cases the response times will be far below the above. Our aim is to respond to any type of failure within 5 minutes.

Security of the Primary and Secondary Array

The security configuration at the data centre comprises two dedicated firewalls configured in tandem for fault tolerance. They are locked down to only allow web traffic (Ports 80 and 443) from public internet address. All other traffic is blocked to prevent unauthorised access to critical servers.

Web traffic is being routed through a ModSecurity Web Application Firewall, providing another level of protection as public web access does not have direct access to the application servers.

There is access permitted from specific IP addresses to specific ports and servers for management by Propeller Studios and their strategic partners. Communication between servers takes place on an internal private network, not connected to the public internet. The Storage Area Network is also completely offline with no direct internet access.

Fire drills and audits of the system

We have developed a comprehensive and robust series of fire drills and simulated disaster recovery events that are undertaken at planned periods throughout the year.

The table below details these arrangements:-

Monthly fire drill events, reports and audits	Outcomes
Review of the monthly hardware inspection sheets for all hardware that makes up both the primary and secondary array completed on the Companies behalf by the service engineer. Monthly inspections are conducted remotely, using our computers own monitoring systems.	The purchase or upgrade of the system based upon decisions reached by the Managing Director, Digital Director and Application Programming Director ensuring a robust process to identify and replace at risk items.
Review of the systems performance report during the month, identifying any concerns and suggestions for improvement.	The purchase or upgrade of the system based upon decisions reached by the Managing Director, Digital Director and Application Programming Director ensuring that the systems performance matches or exceeds the service agreements pledges to clients
Monthly back up data integrity audit between the	A compliance report provided from our engineers

primary and secondary array and between San units of the Primary array.	confirming the successful replication of data between primary and secondary arrays and duplication of data between the SAN units of the primary array.

Quarterly fire drill events, reports and audits	Outcomes
Pre notified testing of the primary array failover capability.	A rigorous examination of the primary and secondary arrays capacity to function when an item of component hardware failure is simulated. The event is supported by a detailed report, highlighting any concerns or suggestions for improvement which are considered and actioned where required.
Half yearly fire drill events, reports and audits	**Outcomes**
Physical inspection of the hosting facilities and inspection of the fire drill records of the strategic partner to ensure compliance with the arrangements.	Completed audit inspection form completed by the Managing Director
Physical inspection of the Intranet providers facilities and inspection of the fire drill records of the strategic partner to ensure compliance with the arrangements.	Completed audit inspection form completed by the Managing Director

EasyPQQ and EasyBOP client access to their own data

Registered users of either application can only ever see the data stored in their own company account. Both applications core logic architecture has been designed to run as a multi-user environment from their inception. Data segregation is enforced through a unique client identifier and is persistent through the application programming logic, the database table relationships, and the file system structure.

Application logic data segregation

Client login sessions are validated on each major page and script, including script-helpers and function library pages. The underlying rule is to check and validate the client's login session prior to any code execution that returns (or potentially makes visible) sensitive data that related to individual specific clients.

Should the client session become corrupt or malformed in any way, the system will flag an error and realise that the client's session is no longer valid. In this case, the client is forcefully logged-out of Intranet where they may then log back in.

An example of a forced log-out may occur if a client tampers with query-string variables while answering a question. The applications will detect an illegal relationship between client and document and force a log-out.

In addition to this validation, client data segregation is enforced multiple times with each identity variable forming a 'chain' back to the client's identity as the source of the validation. If this chain fails, the client is either logged-out, or blank data is purposely returned to the screen.

Database information segregation
This is enforced in the standard database architecture of primary key relationships. The client's unique identifier is used as the basis for most data tables, with complex relationships ultimately forming paths that resolve back down to the client's unique identifier.

File system segregation
Both applications handles file references using the client's unique identifier. For example, File Manager uploads are segregated in to separate physical folders on a per client basis. This ensures Client A's files do not mix with Client B's on any level.

At times the applications will need to generate temporary files. These are always generated with temporary file names which include the client's unique identifier, as well as a time stamp number value down to micro-seconds.

Penetration Testing
Penetration testing is carried out on a monthly basis in order to assess the security of our networks and applications. The results of the penetration tests are reviewed on a monthly basis during the server committee meeting and remedial actions taken, as and when required. Because of the nature of the internet, new threats are constantly evolving and our policy ensures that we rigorously monitor the situation and take preemptive and proactive steps to ensure that we are prepared for all eventualities.

Encryption at rest
All data stored within our applications is encrypted at rest. This means that in the unlikely event that our security precautions are breached, any data extracted from our systems will be unintelligible to the agency stealing it.

Our approved procedure for providing auditable customer support
The mechanism by which we access user accounts, to diagnose bugs or provide assistance during implementation periods, is via a named user account(s) within your security module. The name of the account is generally **Propeller Consultant** or it might be a specific staff name depending upon your requirements. This is set up by us when you subscribe to the product.

In this way we can control access to your systems, and ensure that the details are only ever available to approved personnel within our organisation. It also provides you with visibility of the actions carried out by our customer support staff and any information that they have downloaded from your system. The reports are available in the staff card of our user(s).

We recommend that you manage the account(s) by deactivating it during periods when support is not required. The controls for this are in the security module. In this way, access to the system by Propeller Customer Services staff is impossible without you first opening the connection.

To be effective it should be a super user account with the highest levels of access to the system. You can of course change the access level yourselves but it will limit our ability to quickly diagnose issues and resolve them on your behalf.

To be clear, our support staff are strictly prohibited from providing password information to customers either verbally or by electronic communication.

Data protection and security policy

The Company has implemented policies which govern our approach to Data Protection and Data Security.

The scope of these arrangements is to ensure compliance with all statutory requirements in respect of the Data Protection Act and the General Data Protection Regulations, and to ensure that the systems required to manage its own systems, and that of its clients, are managed in a professional and robust way.

The aim of these policies is to ensure that Propeller Studios provides them optimum environment for the custody of its, and clients', data and to ensure that it remains safe, available and properly managed at all times

A copy of the policy and the registration certificate is attached at the end of this document.

Restitution of Data

Upon termination of a contract with The Company, client data will be stored for a maximum of three months, should the client wish to reinstate their user licence. Following the three month period, the data will be deleted from our servers and will be permanently irretrievable. In regards to backup, The Company's client's data is stored on a rotating seven day backup system therefore no historic data exists beyond the seven day period.

ISO27001 accreditation

The Company recognises that data security is an important aspect of it's business and has gained accreditation for ISO27001. Our data security processes and procedures are independently audited by third party consultants on an annual basis. A copy of the accreditation document is also provided with this document.

Propeller Reference Number	P0011
Version	V5
Document Owner	Andy Hammond
Date Last reviewed	30/09/2018
Date of Next Review	30/09/2019

British Assessment Bureau

Certification is conditional on maintaining the required performance standards throughout the certified period of registration
The British Assessment Bureau, 30 Tower View, Kings Hill, Kent, ME19 4UY

The management system of Certificate Number **185161**

Propeller Studios Ltd

1st Floor, Alexander House Business Centre, 40a Wilbury Way, Hitchen, Hertfordshire, SG4 0AP

has been assessed and certified as meeting the requirements of

BS EN ISO/IEC 27001:2017

for the following activities

Pre Qualification and tender writing consultancy and IT software provider

Further clarifications regarding the scope of this certificate and the applicability of requirements may be obtained by consulting the certifier.

Valid from

Initial Certification: 26 January 2015
Latest Issue: 26 January 2018
Expiry Date: 25 January 2021
subject to annual assessments

Authorised by

Jonathan Chapman
Chief Executive

UKAS MANAGEMENT SYSTEMS 8289

www.british-assessment.co.uk

To validate authenticity a holographic security foil is printed in the bottom right corner of the original certificate
To confirm the 'Live Status' of this certificate please use the 'Certificate Verification' tool located at www.british-assessment.co.uk

Information Commissioner's Office

Upholding information rights

Wycliffe House, Water Lane, Wilmslow, Cheshire SK9 5AF
T. 0303 123 1113 F. 01625 524510
www.ico.org.uk

Certificate

Organisation Name:

PROPELLER STUDIOS LIMITED

Reference number:

Z8231587

Tier:

Tier 1

Start date:

13 October 2003

End date:

12 October 2019

Data Protection Officer

PROPELLER

Propeller Studios Ltd,
First Floor, Alexander House Business Centre,
40a Wilbury Way, Hitchin, Hertforshire SG4 0AP

Tel: +44 (0)1462 440077